BY ORDER OF THE COMMANDER

AIR FORCE SPECIAL OPERATIONS COMMAND INSTRUCTION 10-701

22 JUNE 2006

Operations

OPERATIONS SECURITY (OPSEC)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **www.e-publishing.af.mil**, for downloading or ordering.

RELEASABILITY: There are not releasability restrictions on this publication.

OPR: HQ AFSOC/A3I

Certified by: HQ AFSOC/A31
(Lt Col James K. Sikes)

Supersedes AFSOCI10-1101, 1 January 1998
and HOI31-401, 1 June 2002

Pages: 57

This instruction implements AFI 10-701, *Operations Security (OPSEC)*, replaces AFSOCI 10-1101, *Operations Security (OPSEC)* and HOI 31-401, *Shredding Procedures for HQ AFSOC*. It provides guidance for all AFSOC personnel and supporting contractors in implementing, maintaining and executing the command's OPSEC program. It describes the OPSEC programs and discusses integration of OPSEC into AFSOC plans, operations and support activities. The reporting requirements in this publication are exempt from licensing in accordance with AFI 33-324, paragraph 2.11.1., *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections*. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 37-123 (will convert to AFMAN 33-363), *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at **https://afrims.amc.af.mil/**. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF IMT 847, *Recommendation for Change of Publication*, route AF IMT 847s from the field through the appropriate functional's chain of command. This publication applies to the Air National Guard (ANG) only when activated in accordance with United States Code Title 10. This publication does not apply to the Air Force Reserve Command (AFRC).

SUMMARY OF CHANGES

This document is substantially revised and must be completely reviewed. It integrates new Air Force Doctrine Document 2-5, *Information Operations,* and updates the definition of OPSEC to coincide with Joint Publication (JP) 3-54, *Joint Doctrine for Operations Security*. It introduces the OPSEC Coordinator position at the directorate-level and below wing-level and lays out the duties and responsibilities for all levels of OPSEC within the AFSOC organizational structure. It also places related security disciplines into a table for ease of use, links OPSEC risk assessment to Operational Risk Management (ORM), provides specific requirements for both training and assessment, defines AFSOC critical information, establishes a destruction of sensitive but unclassified material requirement (HQ AFSOC specific policy included) and describes the process for requesting Electronic Systems Security Assessments and using DD Form 254, *DOD Contract Security Classification Specification*, for AFSOC contracts.

Chapter 1

INTRODUCTION

1.1. General. OPSEC is a military capability within Information Operations (IO). IO is the integrated employment of three operational elements: influence operations (Influence Ops), electronic warfare operations (EW Ops), and network warfare operations (NW Ops). All three contribute to the integrated air, space, and information operational plan to disrupt, corrupt, or change targeted human and automated decision-making while protecting our own. Influence Ops employ core military capabilities of psychological operations (PSYOP), OPSEC, military deception (MILDEC), counterintelligence (CI) operations, public affairs (PA) operations and counterpropaganda operations to affect behaviors, protect operations, communicate commander's intent and project accurate information to achieve desired effects across the cognitive battlespace. OPSEC protects friendly operations and efforts to influence the adversary's behavior.

1.2. Definition. OPSEC is a process of identifying, analyzing and controlling critical information indicating friendly actions attendant to military operations and other activities to:

1.2.1. Identify those actions that can be observed by adversary intelligence systems,

1.2.2. Determine what indicators adversary intelligence systems might obtain that could be interpreted or pieced together to derive CRITICAL INFORMATION in time to be useful to adversaries, and

1.2.3. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation (JP 3-54).

1.2.4. OPSEC is a process and not a collection of specific rules and instructions that can be applied to every operation. OPSEC must be closely integrated and synchronized with other Influence Ops capabilities and all aspects of the protected operations.

1.3. Characteristics of OPSEC. The goal of OPSEC is to identify information and observable activities (indicators) relating to mission capabilities, limitations and intentions in order to prevent exploitation by our adversaries. OPSEC methodology provides a step-by-step analysis of our operations and behavior from an adversary's perspective, thereby assessing how vulnerabilities might be exploited. Information that adversaries need to achieve their goals constitutes critical information about our operations or programs. By identifying and protecting this critical information, the OPSEC process becomes a positive, proactive means by which adversaries are denied an important advantage.

1.3.1. Operational effectiveness is enhanced when commanders and other decision-makers apply OPSEC from the earliest stages of planning. OPSEC involves a series of analysis to examine the planning, preparation, execution and post execution phases of any activity across the entire spectrum of military action and in any operational environment. OPSEC analysis provides decision-makers with a means of weighing how much risk they are willing to accept in particular operational circumstances in the same way as ORM allows commanders to assess risk in mission planning. In fact, OPSEC can be referred to as information risk management.

1.3.2. OPSEC must be closely coordinated with other security disciplines (see **Table 1.1.**) as applicable. The primary focus of OPSEC analysis is to deny exploitation of open source information and observable activities. These sources are generally unclassified and difficult to control.

Table 1.1. Related Security Disciplines and Source Documentation

Anti-Terrorism/Force Protection Program	AFI 10-245
Communications Security User Requirements	AFI 33-211
Electronic Mail (E-mail) Management and Use	AFI 33-119
Emissions Security	AFI 33-203
Freedom of Information Act (FOIA)	DODR 5400.7/AF SUP 1999
Industrial Security	AFPD 31-6/AFI 31-601
Information Protection	AFPD 33-2
Information Security	AFPD 31-4/AFI 31-401
Network and Computer Security	AFI 33-202
Personnel Security	AFPD 31-5/AFI 31-501
Physical Security	AFPD 31-1
Privacy Act Information	AFI 33-332
Public Affairs Policies and Procedures	AFI-35-101, Chapters 15 and 18
Reporting COMSEC Deviation	AFI 33-212
Technology and Acquisition Systems Security Program Protection	AFPD 63-17
Telecommunications Monitoring and Assessment Program	AFI 33-219
Web Management and Internet Use	AFI 33-129

1.3.3. OPSEC provides a method of identifying our critical information and denying or controlling an adversary’s access to that information. OPSEC enables friendly force information superiority by neutralizing adversary information collection activities.

1.3.3.1. OPSEC will be employed with other complementary IO activities to obtain maximum effectiveness. Commanders and their planners should utilize all capabilities within IO, including OPSEC, in a synchronized effort to influence the perceptions and affect decision-making of an adversary. For example, a known OPSEC vulnerability may be used to deliver a deception message or psychological operations theme, instead of simply correcting or mitigating the vulnerability. In this case, the use of the discovered vulnerability would be considered the appropriate application of an OPSEC measure.

1.4. Air Force Special Operations Command (AFSOC) OPSEC. AFSOC implements OPSEC in all functional areas. Commanders are responsible for OPSEC awareness throughout their organizations and for integrating the OPSEC process throughout all mission areas. AFSOC commanders and decision-makers will employ OPSEC during mission planning, mission support, force execution and throughout the acquisition process. OPSEC will be incorporated into day-to-day activities to ensure a seamless transition to contingency operations.

1.4.1. OPSEC issues must be integrated into every aspects of planning and execution of all AFSOC operations. OPSEC assists in the protection of AFSOC capabilities and intentions by degrading an adversary's knowledge of and subsequent ability to attack our forces or counter our operations. Embedding OPSEC into campaign planning and force execution maximizes mission effectiveness.

1.4.2. OPSEC supports AFSOC research, development, testing and evaluation (RDT&E) through the reduction of compromised technology and proprietary information. Acquisition organizations that fail to implement OPSEC could unintentionally reveal critical program information, ultimately increasing operational risk as potentially compromised systems are fielded.

1.4.3. AFSOC OPSEC is an integral process of force protection, helping protect service members, civilian employees, family members, facilities and equipment at all locations and in all situations. Force protection relies heavily on OPSEC as a means of denying targeting information to terrorists and other adversaries. Since force protection safeguards the AFSOC's most precious asset—***people,*** it is critical that OPSEC be applied throughout the Command.

1.5. The OPSEC Process. The OPSEC process consists of five distinct steps: 1) identification of critical information, 2) analysis of threats, 3) analysis of vulnerabilities, 4) assessment of risk, and 5) application of appropriate OPSEC measures.

Chapter 2

AIR FORCE SPECIAL OPERATIONS COMMAND OPSEC PROGRAM

2.1. Purpose. The purpose of the AFSOC OPSEC program is to provide commanders with standardized policy and to facilitate effective OPSEC programs by promoting general understanding and awareness regarding the integration and application of OPSEC. An overall AFSOC OPSEC Program Manager (PM) is identified within the headquarters staff to advise on the integration of OPSEC into command-wide efforts and to develop policy and guidance that provides coordination, training, education and recognition for AFSOC-wide OPSEC programs.

2.2. Roles And Responsibilities. All AFSOC organizations must integrate OPSEC into their planning and develop OPSEC plans (wing-level or equivalent) to ensure a viable OPSEC program is created and maintained that identifies the organization's critical information and indicators and develops OPSEC measures to counter their inherent vulnerabilities. AFSOC units will integrate OPSEC into military strategy, operational and tactical planning and execution, all support activities, all contingency, combat and peacetime operations and exercises, communications/computer architectures and processing, weapons systems RDT&E, AFSOC specialized training, inspections, acquisition and procurement, and professional military education programs. Although the OPSEC program helps commanders make and implement decisions, the decisions are the commander's responsibility. Commanders must understand the risk to the mission and then determine which OPSEC measures are required.

2.2.1. Headquarters, AFSOC Responsibilities. The Commander, AFSOC is the office of primary responsibility (OPR) for the AFSOC OPSEC program. AFSOC/CC is responsible for coordinating OPSEC policy, doctrine, strategy and investment priorities within the command. Other organizations having individual responsibilities for elements of OPSEC will coordinate with the HQ AFSOC OPSEC PM to ensure the consistent and standardized application of OPSEC policy and guidance.

2.2.1.1. Commander, Air Force Special Operations Command will: (**Note:** Commanders may delegate authority for OPSEC program management, but retain responsibility for risk management decisions and the overall implementation of OPSEC measures.)

2.2.1.1.1. In coordination with HQ AF/A3I and USSOCOM/J39, be responsible for OPSEC implementation, posture and operations within the command and all assigned units. Additionally, he is responsible for enforcing OPSEC policies and directives, ensuring that OPSEC plans and programs at every echelon are supported by the existing intelligence organizations/infrastructure at those levels.

2.2.1.1.2. Designate a full-time primary and alternate PM, in writing (see AFSOC OPSEC Plan for letter template). The PM may be military (Officer or NCO) or DOD civilian (GS-12 or above) having or able to obtain a Top Secret clearance. Forward a copy of the appointment letter to HQ AF/A3I.

2.2.1.1.3. Ensure an OPSEC program is developed IAW policy and guidance issued by HQ AF/A3I and USSOCOM/J39 and that all subordinate organizations integrate OPSEC into day-to-day operations. Ensure OPSEC is integrated with other IO activities.

2.2.1.1.4. Ensure OPSEC funding is programmed for all OPSEC training through established budgeting and requirements processes.

2.2.1.1.5. Ensure coordination across organizational boundaries as necessary (both vertically and horizontally) to facilitate consistent application of OPSEC throughout the command.

2.2.1.1.6. Ensure all subordinate units are identifying their critical information for their unit's mission and each operation, activity and exercise whether it be planned, conducted, or supported.

2.2.1.1.7. Ensure all subordinate units are controlling critical information and OPSEC indicators.

2.2.1.1.8. Ensure all subordinate units plan, exercise and implement OPSEC measures as appropriate.

2.2.1.1.9. Ensure OPSEC considerations are integrated into the acquisition cycle and OPSEC considerations are included in Initial Capabilities Documents, Capability Development Documents and inputs to the combatant commanders' Integrated Priority Lists.

2.2.1.1.10. Ensure intelligence and counterintelligence relationships are developed and cultivated as necessary to support OPSEC programs.

2.2.1.1.11. Ensure OPSEC considerations are included in annual unclassified web page reviews and in the approval process for posting new data to the web IAW AFI 33-129.

2.2.1.1.12. Ensure OPSEC considerations are included in PA's review and approval process for the publishing or releasing of information to or that may be viewed by the public (i.e. base newspapers, safety magazines, flyers, web pages, television interviews and information for news articles).

2.2.1.1.13. Ensure mission-oriented OPSEC education and awareness training is provided to all AFSOC personnel within 90 days of initial assignment and then annually thereafter.

2.2.1.1.14. Ensure training of OPSEC PMs at wing-level and above is accomplished within 90 days of appointment, or by the next available class.

2.2.1.1.15. Ensure annual self-assessments are completed.

2.2.1.1.16. Ensure OPSEC vulnerability reports are forwarded to HQ AIA, 67 IOW, Electronic Systems Security Assessment Tasking Cell in a timely manner.

2.2.1.1.17. Ensure policies, supplements or other directions are developed, issued and implemented as required.

2.2.1.1.18. Recommend changes to policies, plans and procedures of the AF and USSOCOM OPSEC Programs to HQ AF/A3I and USSOCOM/J39 Staff.

2.2.1.1.19. Provide oversight, advocacy and act as the management/tasking focal point for the AFSOC Electronic Systems Security Assessment (ESSA) Team (proposed AFSOC ESSA Center) in conducting the Telecommunications Monitoring and Assessment (TMAP) Program.

2.2.2. HQ AFSOC Directorates, AFSOF, Wings, Special Operations Groups (SOGs), FOA and DRUs to include all gained units. At the base/installation level, AFSOC gained units will comply with host base guidance. All AFSOC gained units to include HQ AFSOC directorates will develop effective OPSEC programs that meet the specific needs of their assigned mission.

2.2.2.1. HQ AFSOC Directors will: (**Note:** Commanders may delegate authority for OPSEC program management, but retain responsibility for risk management decisions and the overall implementation of OPSEC measures.)

2.2.2.1.1. In coordination with AFSOC/CC, be responsible for OPSEC implementation, posture and operations within their assigned directorates. Additionally, they are responsible for enforcing OPSEC policies and directives, ensuring that OPSEC plans and programs at every echelon are supported by the existing intelligence organizations/infrastructure at those levels.

2.2.2.1.2. Designate a primary and alternate OPSEC Coordinator, in writing (see AFSOC OPSEC Plan for letter template). The coordinator may be military (Officer or NCO) or DOD civilian having at least a Secret clearance and should have access to SIPRNET. Directors may, at their choosing and based on directorate size, designate more than one primary and alternate OPSEC Coordinator. Forward a copy of the appointment letter to the HQ AFSOC OPSEC PM.

2.2.2.1.3. Ensure an OPSEC program is developed IAW policy and guidance issued by AFSOC/CC or his agent and integrate OPSEC into day-to-day operations. Ensure OPSEC is integrated with other AFSOC IO activities.

2.2.2.1.4. Ensure OPSEC funding is programmed for all OPSEC training through established budgeting and requirements processes.

2.2.2.1.5. Ensure coordination across organizational boundaries as necessary (both vertically and horizontally) to facilitate consistent application of OPSEC throughout the directorate.

2.2.2.1.6. Ensure directorate critical information is identified for the directorate's mission and each operation, activity and exercise whether it be planned, conducted, or supported.

2.2.2.1.7. Ensure directorate is controlling critical information and OPSEC indicators.

2.2.2.1.8. Ensure directorate plans, exercises and implements OPSEC measures as appropriate.

2.2.2.1.9. Ensure OPSEC considerations are integrated into the acquisition cycle and OPSEC considerations are included in Initial Capabilities Documents, Capability Development Documents and inputs to the combatant commanders' Integrated Priority Lists.

2.2.2.1.10. Ensure OPSEC considerations are included in annual unclassified web page reviews and in the approval process for posting new data to the web IAW AFI 33-129.

2.2.2.1.11. Ensure OPSEC considerations are included in the directorate's review and approval process for the publishing or releasing of information to or that may be viewed by the public (i.e. base newspapers, safety magazines, flyers, web pages, television interviews and information for news articles).

2.2.2.1.12. Ensure mission-oriented OPSEC education and awareness training is provided to all assigned personnel within 90 days of initial assignment and then annually thereafter.

2.2.2.1.13. Ensure training of assigned OPSEC coordinators is accomplished within 180 days of appointment, or by the next available class.

2.2.2.1.14. Ensure annual self-assessments are completed.

2.2.2.1.15. Ensure OPSEC vulnerability reports are forwarded to HQ AFSOC OPSEC PM in a timely manner.

2.2.2.1.16. Take an active role in integrating OPSEC into mission plans and day-to-day activities.

2.2.2.2. Wing Commanders will (to include SOGs, FOA and DRUs): (**Note:** Commanders may delegate authority for OPSEC program management, but retain responsibility for risk management decisions and the overall implementation of OPSEC measures.)

2.2.2.2.1. In coordination with HQ AFSOC/A3I, be responsible for OPSEC implementation, posture and operations within their assigned units. Additionally, they are responsible for enforcing OPSEC policies and directives, ensuring that OPSEC plans and programs at every echelon are supported by the existing intelligence organizations/infrastructure at those levels.

2.2.2.2.2. Designate a primary and alternate Wing PM, in writing (see AFSOC OPSEC Plan for letter template). The PM may be military (Officer or SNCO) or DOD civilian (GS-11 or above) having at least a Secret clearance. Forward a copy of the appointment letter to the HQ AFSOC OPSEC PM.

2.2.2.2.3. Ensure an OPSEC program is developed IAW policy and guidance issued by HQ AFSOC/A3I and subordinate units integrate OPSEC into day-to-day operations. Ensure OPSEC is integrated with other wing IO activities.

2.2.2.2.4. Ensure OPSEC funding is programmed for all OPSEC training through established budgeting and requirements processes.

2.2.2.2.5. Ensure coordination across unit boundaries as necessary (both vertically and horizontally) to facilitate consistent application of OPSEC throughout the wing.

2.2.2.2.6. Ensure all subordinate units are identifying their critical information for their unit's mission and each operation, activity and exercise whether it be planned, conducted, or supported.

2.2.2.2.7. Ensure all subordinate units are controlling critical information and OPSEC indicators.

2.2.2.2.8. Ensure all subordinate units plan, exercise and implement OPSEC measures as appropriate.

2.2.2.2.9. Ensure OPSEC considerations are integrated into the acquisition cycle and OPSEC considerations are included in Initial Capabilities Documents and Capability Development Documents.

2.2.2.2.10. Ensure intelligence and counterintelligence relationships are developed and cultivated as necessary to support OPSEC programs.

2.2.2.2.11. Ensure OPSEC considerations are included in annual unclassified web page reviews and in the approval process for posting new data to the web IAW AFI 33-129.

2.2.2.2.12. Ensure OPSEC considerations are included in PA's review and approval process for the publishing or releasing of information to or that may be viewed by the public (i.e. base papers, safety magazines, flyers, web pages, television interviews and information for news articles).

2.2.2.2.13. Ensure mission-oriented OPSEC education and awareness training is provided to all assigned personnel within 90 days of initial assignment and then annually thereafter.

2.2.2.2.14. Ensure training of OPSEC PMs at wing-level is accomplished within 90 days of appointment, or by the next available class.

2.2.2.2.15. Ensure annual self-assessments are completed.

2.2.2.2.16. Ensure OPSEC vulnerability reports are forwarded to HQ AFSOC OPSEC PM in a timely manner.

2.2.2.2.17. Ensure policies, supplements or other directions are developed, issued and implemented as required.

2.2.2.2.18. Take an active role in integrating OPSEC into mission plans and day-to-day activities.

2.2.3. The AFSOC Chief Information Officer (AFSOC/A6-CIO). The AFSOC Chief Information Officer is the OPR for information assurance policy, guidance and operational oversight. He is responsible for ensuring that AFSOC OPSEC principles and practices are correctly reflected in the AFSOC Enterprise Architecture. AFSOC/A6-CIO is also responsible for ensuring interoperability of information warfare systems and concepts.

2.3. OPSEC Reporting. The Air Force OPSEC program's reporting requirements include two types of time-sensitive reports: See AFI 10-701 for more details.

2.4. Air Force OPSEC Awards Program. The annual Air Force OPSEC Awards Program provides recognition of Air Force OPSEC professionals. See AFI 10-701 for more details.

Chapter 3

UNIT OPSEC PROGRAMS

3.1. Purpose and Composition. AFSOC OPSEC programs support the commander's efforts to accomplish a successful and effective mission. Each program is composed of an OPSEC PM or coordinator, OPSEC plans, funding, training, assessments and feedback. AFSOC OPSEC programs must have the following critical aspects: commander involvement, operational focus, integration, coordination and assessment.

3.1.1. Commander Involvement. Commanders are responsible for ensuring OPSEC is integrated into day-to-day operations. Commanders may delegate authority for their OPSEC program management, but retain responsibility for risk management decisions and the overall implementation of OPSEC measures.

3.1.2. Operational Focus. The AFSOC OPSEC program is an operations program and its goals are information superiority and optimal mission effectiveness. The emphasis is on OPERATIONS and the assurance of effective mission accomplishment. The unit OPSEC PM and Coordinator should reside in the operations or plans element of an organization or report directly to the unit commander to ensure effective implementation across organizational and functional lines. However, for those units with no traditional operations or plans element, the commander must decide the most logical area to place management and coordination of the unit's OPSEC program while focusing on operations and the mission of the unit.

3.1.3. Integration and Coordination. PMs and coordinators will integrate OPSEC into all organizational plans and activities. Staff elements and supporting organizations will ensure OPSEC is appropriately incorporated at the earliest possible time into all operations plans (OPLANs), concept plans (CONPLANs), concept of operations (CONOPs), operations orders (OPORDs), exercise plans, Initial Capability Documents (ICD), Capability Development Documents (CDD), Initial Requirement Documents (IRD), program protection plans (PPP), operating procedures and other plans and activities to ensure consistent control of critical information and OPSEC indicators. All applicable contracts, Statements of Work (SOW), Requests for Proposals (RFP), Contract Security Classification Specification (DD Form 254) and similar documentation will contain specific statements or requirements that address security criteria for protecting critical information and OPSEC indicators. All OPSEC PMs and coordinators will add an OPSEC section to each respective annex to all organizational plans. The appropriate functional area OPSEC PM or coordinator will evaluate all appropriate contractual documents regarding OPSEC and will work with the local contracting office to ensure the intent of the program is met.

3.1.3.1. AFSOC OPSEC must be an integral part of an overall IO effort. This applies to other IO and Influence Ops functions that also protect friendly information and that may influence the adversary's decision-making process. For example, integration of OPSEC and Public Affairs is particularly important as the need to protect critical information must be balanced against the desire to provide information to the public. The OPSEC PM or coordinator will maintain copies of all applicable Public Affairs guidance and ensure the Public Affairs office is aware of critical information elements.

3.1.3.2. AFSOC OPSEC is integrated into the Air Force Special Operations Forces (AFSOF) Air Operations Center (AOC) through the IO Specialty Team. IO Specialty Team OPSEC coordinators/planners work within the AOC to ensure planning and execution of air, space and IO incorporate OPSEC. IO Specialty Team OPSEC coordinators/planners work with the rest of the IO Specialty Team to integrate OPSEC with other IO activities. When an AOC is formed, IO Specialty Team OPSEC coordinators/planners become the focal point for integrating the activities of supporting elements OPSEC PMs and coordinators. This ensures the Commander, AFSOF, has a coherent OPSEC effort across all units.

3.1.3.3. Each wing/SOG will have a written OPSEC plan. OPSEC PMs will follow AFSOC OPSEC Plan format in developing their own, uniquely tailored OPSEC Plan.

3.1.4. Assessment. Assessment of your program is critical to its continued grow and success. There are several assessment programs that can be used to check the health of your OPSEC program. Here are two that are easy and inexpensive to use.

3.1.4.1. Self-Assessment. PMs and coordinators will accomplish a self-assessment of their OPSEC Program using this instruction and the self-assessment checklist located in **Attachment 3**, NLT 30 September of each year.

3.1.4.2. Program Assessment. The HQ AFSOC OPSEC PM, wing and wing-equivalent PMs will accomplish a program assessment of their assigned unit's OPSEC programs using AFI 10-701, AFSOCI 10-701, and the self-assessment checklist located in **Attachment 3** biennially (every two years).

3.2. AFSOC OPSEC PMs. OPSEC PMs and alternates will be assigned at wing- or wing-equivalent level (SOGs, FOA, and DRUs) and above. Organizations at wing or wing-equivalent level (and above) must appoint an OPSEC PM and alternate, in writing (see AFSOC OPSEC Plan for letter template). The wing or wing-equivalent level PM can come from any organizational level the commander deems appropriate. For example, the wing PM may actually be assigned at the Operations Group level, but performs OPSEC PM duties in direct support of the entire wing. The respective wing or wing-equivalent commander will sign appointment letters. Letters of appointment must be forwarded to the HQ AFSOC OPSEC PM. OPSEC PMs should be assigned for a minimum of 18 months to allow the PM to obtain proper training and experience. The OPSEC PM requires a security clearance appropriate to the mission and function of the organization, but no lower than Secret. Wing or wing-equivalent (and above) PMs require SIPRNET access to read OPSEC Advisory Reports, whether in their work center or from another terminal on the installation. Wing or wing-equivalent OPSEC PMs may also serve as the lead Influence Ops and IO Manager. Wing (host unit) OPSEC PMs will coordinate OPSEC with tenant unit OPSEC PMs and/or coordinators. AFSOC tenant unit OPSEC PMs will closely coordinate and integrate with host wing OPSEC initiatives; however, administrative oversight of the tenant unit's program still resides with HQ AFSOC/A3I. If the host organization has an OPSEC working group, the tenant unit PM will seek representation in it.

3.2.1. HQ AFSOC OPSEC PM duties include, but are not limited to:

3.2.1.1. Develop, coordinate and manage the AFSOC OPSEC Program, OPSEC Plan and implementation of OPSEC into day-to-day operations throughout the command.

3.2.1.2. Act as primary advisor to the AFSOC/CC on all OPSEC matters.

3.2.1.3. Develop and implement the commander's OPSEC policies and command's critical information list (CIL).

3.2.1.4. Develop procedures to ensure critical information, OPSEC indicators and sensitive activities are controlled.

3.2.1.5. Forward a copy of the appointment letter to HQ AF/A3I.

3.2.1.6. Incorporate OPSEC into command plans, exercises, activities and command-to-command agreements.

3.2.1.7. Incorporate OPSEC lessons learned from command/unit operations and exercises as well as other operations and exercises into the command's planning process. Forward lessons learned to appropriate depositories.

3.2.1.8. Develop, issue and implement policies, supplements or other directions as required.

3.2.1.9. Provide management, development and oversight of appropriate OPSEC training and conduct training as required. Coordinate with the 39 IOS for AF OPSEC training, general education and course quotas to the AF OPSEC Course. Attend AF OPSEC course within 90 days of appointment, or by the next available class.

3.2.1.10. Develop and maintain an effective working relationship with Intelligence and OSI CounterIntelligence and request additional intelligence and counterintelligence support to meet OPSEC program requirements.

3.2.1.11. Ensure OPSEC considerations are included in command PA's review and approval process for the publishing or releasing of information to or that may be viewed by the public (i.e. safety magazines, flyers, web pages, television interviews and information for news articles). Conduct reviews as required.

3.2.1.12. Ensure OPSEC reviews are conducted on all command web pages prior to the information being placed, updated, or modified on the web page and annually thereafter.

3.2.1.12.1. Ensure OPSEC reviews consider the proliferation of internet/web-based bulletin boards and web logs (blogs) and evaluate the risk presented by web content in annual OPSEC assessments.

3.2.1.12.2. Conduct reviews as required.

3.2.1.13. Integrate OPSEC into IO; Influence Ops, and other supporting capabilities.

3.2.1.14. Ensure annual OPSEC self-assessments are conducted by subordinate units and results forwarded to HQ AFSOC by 15 October of each year. Coordinate, facilitate and conduct OPSEC program assessments on HQ AFSOC directorate and subordinate units biennially (every two years).

3.2.1.15. Consolidate and submit all self-assessment report to the Air Force OPSEC PM (HQ AF/A3I) NLT 15 Nov each year. This report will contain training metrics of initial and annual training for all subordinate units, the number of vulnerability reports forwarded to the HQ AIA, 67 IOW, Electronic Systems Security Assessment Tasking Cell, number and type of survey/assessments received by subordinate units (command survey, TMAP support, Multi-Discipline Vulnerability Assessment (MDVA), and any other information deemed of OPSEC importance.

3.2.1.16. Participate in all applicable working groups (i.e. Threat, Force Protection, Anti-Terrorism, Information Operation, Influence Ops, etc.).

3.2.1.17. Submit OPSEC vulnerability reports to HQ AIA, 67 IOW, Electronic Systems Security Assessment Tasking Cell in a timely manner.

3.2.1.18. Ensure OPSEC is integrated into all acquisition programs and contractor support documents/agreements.

3.2.1.19. Conduct Staff Assistance Visits (SAV) to all subordinate units as required or requested.

3.2.1.20. Serve as the command focal point for management and scheduling of all AFSOC Electronic Systems Security Assessment (ESSA) requirements.

3.2.1.21. Prioritize and consolidate vulnerability assessment requirements (i.e., MDVAs and/or formal surveys) for the wings and subordinate units. Forward requirements to ACC/A3I for scheduling.

3.2.1.22. Submit an annual budget requirement to the Air Staff for inclusion into the AF Program Objective Memorandum (POM) process. OPSEC capabilities and solutions requirements will be identified through the IO Capabilities Plan.

3.2.2. Wing-level OPSEC PMs duties include, but are not limited to: (The following responsibilities are not all inclusive. The HQ AFSOC OPSEC PM will assign additional OPSEC responsibilities pertinent to individual mission requirements.)

3.2.2.1. Develop, coordinate and manage the Wing's OPSEC Program, OPSEC Plan and implementation of OPSEC into day-to-day operations throughout the wing.

3.2.2.1.1. Post OPSEC multimedia aids throughout Wing facilities.

3.2.2.1.2. Ensure primary and alternate OPSEC coordinators have been selected for each group and squadron and their pictures and phone numbers are posted throughout their assigned facilities.

3.2.2.1.3. Ensure each unit develops a unit specific CIL and post a copy at each work station.

3.2.2.1.4. Conduct biennially (every two years) OPSEC assessments of respective organization's OPSEC program.

3.2.2.2. Act as primary advisor to the wing commander on all OPSEC matters.

3.2.2.3. Develop and implement the commander's OPSEC policies and wing's CIL. Review the wing's CIL during Jan of each year and forward the new/updated list to the HQ AFSOC OPSEC PM by 31 Jan of each year.

3.2.2.4. Develop procedures to ensure wing critical information, OPSEC indicators and sensitive activities are identified and controlled.

3.2.2.5. Incorporate OPSEC into wing plans, exercises, activities and wing-to-tenant/local community agreements.

3.2.2.6. Incorporate OPSEC lessons learned from wing/group and unit operations and exercises as well as other operations and exercises into the wing's planning process. Forward lessons learned to appropriate depositories.

3.2.2.7. Develop, issue and implement policies, supplements or other directions as required.

3.2.2.8. Provide management, development and oversight of appropriate OPSEC training and conduct/attend training as required. Attend AF OPSEC course within 90 days of appointment, or by the next available class.

3.2.2.8.1. Ensure all wing personnel receive initial (within 90 days of arrival at duty station) and annual OPSEC training and maintain documentation of personnel trained for both initial and annual training.

3.2.2.8.2. Coordinate with other wing security PMs (e.g., COMSEC, COMPUSEC, Force Protection, INFOSEC, and Personnel Security) to incorporate OPSEC concepts and lessons learned into their security training sessions.

3.2.2.9. Develop and maintain an effective working relationship with Intelligence and OSI CounterIntelligence and request additional intelligence and counterintelligence support to meet OPSEC program requirements.

3.2.2.10. Ensure OPSEC considerations are included in wing PA's review and approval process for the publishing or releasing of information to or that may be viewed by the public (i.e. safety magazines, flyers, web pages, television interviews and information for news articles). Conduct reviews as required.

3.2.2.11. Ensure OPSEC reviews are conducted on all wing web pages prior to the information being placed, updated, or modified on the web page and annually thereafter.

3.2.2.11.1. Ensure OPSEC reviews consider the proliferation of internet/web-based bulletin boards and web logs (blogs) and evaluate the risk presented by web content in annual OPSEC assessments.

3.2.2.11.2. Conduct reviews as required.

3.2.2.12. Integrate OPSEC into IO, Influence Ops and other supporting capabilities.

3.2.2.13. Ensure annual OPSEC self-assessments are conducted by subordinate units and results forwarded to HQ AFSOC OPSEC PM by 15 October of each year. Coordinate, facilitate and conduct OPSEC program assessments on wing staff and subordinate units biennially (every two years).

3.2.2.14. Establish and chair wing OPSEC Working Group (OWG) meetings on a quarterly basis.

3.2.2.14.1. Solicit, publish, and distribute agenda items one week prior to each meeting.

3.2.2.14.2. Record, publish, and distribute minutes NLT two weeks after the meeting. Send a copy of these minutes to the HQ AFSOC OPSEC PM.

3.2.2.14.3. Forward OWG recommendations to the appropriate commander for review and approval.

3.2.2.15. Participate in all applicable working groups (i.e. Threat, Force Protection, Anti-Terrorism, Information Operation, Influence Ops, etc.).

3.2.2.16. Submit OPSEC vulnerability reports to HQ AIA, 67 IOW, Electronic Systems Security Assessment Tasking Cell in a timely manner. Info copy HQ AFSOC OPSEC PM on each submission.

3.2.2.17. Ensure OPSEC is integrated into all acquisition programs and contractor support documents/agreements.

3.2.2.18. Conduct Staff Assistance Visits (SAV) to all subordinate units as required or requested.

3.2.2.19. Serve as the wing focal point for management and scheduling of all ESSA requirements.

3.2.2.20. Prioritize and consolidate vulnerability assessment requirements. Request and coordinate MDVAs (act as lead trusted agent for wing), conduct formal surveys for the wing's subordinate units. Forward all outside requirements to HQ AFSOC OPSEC PM for scheduling.

3.2.2.21. Submit an annual budget requirement to the HQ AFSOC OPSEC PM for inclusion into the AFSOC budget process. OPSEC capabilities and solutions requirements will be identified through the AFSOC IO Capabilities Plan.

3.2.2.22. Establish and maintain a wing OPSEC continuity binder (See AFSOC OPSEC Plan)

3.3. AFSOC OPSEC Coordinators. OPSEC coordinators and alternates will be assigned for each subordinate unit (down to squadron-level) under wing or wing-equivalent level to work with their wing PMs, in writing. AFSOC/CC also requires coordinators within HQ AFSOC directorates. The respective commander or HQ AFSOC Directors will sign appointment letters. Letters of appointment must be forwarded to respective HHQ OPSEC PM. Coordinators can come from any area of the organizational the commander/director deems appropriate and should work directly for the commander/director. All OPSEC coordinators will maintain an appropriate clearance, but a minimum of Secret is required. HQ AFSOC Directorate OPSEC coordinators require SIPRNET access to read OPSEC Advisory Reports, whether in their work center or from another terminal within the directorate. If possible, OPSEC coordinators should not have any other additional duties. AFSOC tenant unit coordinators will closely coordinate and integrate with host wing OPSEC initiatives; however, administrative oversight of the tenant unit's program still resides with their respective wing PM or HQ AFSOC/A3I. If the host organization has an OPSEC working group, the tenant unit Coordinator will seek representation in it.

3.3.1. HQ AFSOC Directorate OPSEC Coordinators will: (The following responsibilities are not all inclusive. The HQ AFSOC OPSEC PM will assign additional OPSEC responsibilities pertinent to individual mission requirements.)

3.3.1.1. Develop, coordinate and manage an OPSEC Program for their directorate.

3.3.1.1.1. Implement and execute OPSEC utilizing director and HQ AFSOC OPSEC PM policy and guidance.

3.3.1.1.2. Implement OPSEC into day-to-day operations throughout the directorate.

3.3.1.1.3. Develop a directorate specific CIL and post a copy at each work station.

3.3.1.2. Act as primary advisor to the director on all OPSEC matters.

3.3.1.3. Develop and implement the director's OPSEC policies and directorate's CIL. Review the directorate's CIL during Jan of each year, and forward the new/updated list to the HQ AFSOC OPSEC PM by 31 Jan of each year.

3.3.1.4. Develop procedures to ensure directorate critical information, OPSEC indicators and sensitive activities are identified and controlled.

3.3.1.5. Forward a copy of the appointment letter to HQ AFSOC OPSEC PM.

3.3.1.6. Incorporate OPSEC into directorate plans, exercises, activities and command-to-command agreements.

3.3.1.7. Incorporate OPSEC lessons learned from directorate operations and exercises as well as other operations and exercises into the director's planning process. Forward lessons learned to appropriate depositories through the HQ AFSOC OPSEC PM.

3.3.1.8. Implement policies, supplements or other directions as required.

3.3.1.9. Conduct/Attend appropriate OPSEC training as required.

3.3.1.9.1. Ensure all directorate personnel receive directorate-specific and annual OPSEC training and maintain documentation of personnel trained for both initial and annual training.

3.3.1.9.2. Attend AF OPSEC course within 120 days of appointment, or by the next available class.

3.3.1.10. Ensure OPSEC considerations are included in directorate review and approval process for the publishing or releasing of information to or that may be viewed by the public (i.e. safety magazines, flyers, web pages, television interviews and information for news articles). Conduct reviews as required.

3.3.1.11. Conduct OPSEC reviews on all directorate web pages prior to the information being placed, updated, or modified on the web page and annually thereafter.

3.3.1.12. Conduct annual OPSEC self-assessment of the directorate's OPSEC program; forward results to the HQ AFSOC OPSEC PM by 15 October of each year.

3.3.1.13. Participate in all applicable working groups as required.

3.3.1.14. Submit OPSEC vulnerability reports to the HQ AFSOC OPSEC PM for submission.

3.3.1.15. Ensure OPSEC is integrated into all acquisition programs and contractor support documents/agreements.

3.3.1.16. Serve as the directorate focal point for all ESSA requirements.

3.3.1.17. Utilize assessment results to correct/resolve/mitigate Web Risk Assessment, Telephone Monitoring Assessment Program (TMAP), Multi-Dimensional Vulnerability Assessment (MDVA), OPSEC survey and other OPSEC assessment findings as required and aid organization OPSEC awareness efforts.

3.3.1.18. Submit an annual budget requirement to the HQ AFSOC OPSEC PM for inclusion into the AFSOC budget process. OPSEC capabilities and solutions requirements will be identified through the AFSOC IO Capabilities Plan.

3.3.1.19. Establish and maintain a directorate OPSEC continuity binder (See AFSOC OPSEC Plan).

3.3.2. Unit OPSEC Coordinators (below Wing level) will: (The following responsibilities are not all inclusive. The Wing OPSEC PM will assign additional OPSEC responsibilities pertinent to their mission.)

3.3.2.1. Implement and execute OPSEC utilizing commander and HHQ OPSEC PM policy and guidance. Implement OPSEC into day-to-day operations throughout the unit.

3.3.2.1.1. Post OPSEC multimedia aids throughout the unit.

3.3.2.1.2. Post your picture and phone number throughout assigned facilities.

3.3.2.1.3. Develop a unit specific CIL and post a copy at each work station.

3.3.2.2. Act as primary advisor to the unit commander on all OPSEC matters.

3.3.2.3. Develop and implement the commander's OPSEC policies and unit's CIL. Review the unit's CIL during Jan of each year, and forward the new/updated list to the wing OPSEC PM by 31 Jan of each year.

3.3.2.4. Develop procedures to ensure unit critical information, OPSEC indicators and sensitive activities are identified and controlled.

3.3.2.5. Forward a copy of the appointment letter to the wing OPSEC PM.

3.3.2.6. Incorporate OPSEC into unit plans, exercises and activities.

3.3.2.7. Incorporate OPSEC lessons learned from unit operations and exercises as well as other operations and exercises into the unit's planning process. Forward lessons learned to appropriate depositories through the wing PM.

3.3.2.8. Implement policies, supplements or other directions as required.

3.3.2.9. Conduct/Attend appropriate OPSEC training as required.

3.3.2.9.1. Ensure all unit personnel receive unit-specific and annual OPSEC training and maintain documentation of personnel trained for both initial and annual training.

3.3.2.9.2. Attend AF OPSEC course or Wing OPSEC PM provided training.

3.3.2.10. Ensure OPSEC considerations are included in unit review and approval process for the publishing or releasing of information to or that may be viewed by the public (i.e. safety magazines, flyers, web pages, television interviews and information for news articles). Conduct reviews as required.

3.3.2.11. Conduct OPSEC reviews on all unit web pages prior to the information being placed, updated, or modified on the web page and annually thereafter.

3.3.2.12. Conduct annual OPSEC self-assessment of the unit's OPSEC program; forward results to the wing OPSEC PM by 1 October of each year.

3.3.2.13. Participate in all applicable working groups as required.

3.3.2.14. Submit OPSEC vulnerability reports to the wing OPSEC PM for submission.

3.3.2.15. Ensure OPSEC is integrated into all unit requested contractor support documents/ agreements.

3.3.2.16. Serve as the unit focal point for scheduling of all ESSA requirements.

3.3.2.17. Utilize assessment results to correct/resolve/mitigate Web Risk Assessment, TMAP, MDVA, OPSEC survey and other OPSEC assessment findings as required and aid organization OPSEC awareness efforts.

3.3.2.18. Establish and maintain a unit OPSEC continuity binder (See AFSOC OPSEC Plan).

3.4. OPSEC Planners. OPSEC planners are personnel who accomplish the duties of an OPSEC Coordinator, but have received specialized planning training (i.e. IO Integration Course, AOC Field Training Unit). OPSEC Planners normally reside within the AFSOF construct. When employed within the AOC, OPSEC Planners function as part of the IO Specialty Team.

3.5. The OPSEC Working Group (OWG). An OWG will be established at wing- or wing-equivalent level and can be established at AFSOC directorate-level to facilitate the AFSOC OPSEC Program. In addition, an ad-hoc OWG should be established for any large-scale operation or exercise. At the wing- or wing-equivalent level, the OPSEC PM will chair the OWG and report directly to the commander. The OWG will ensure the timely and efficient review of activities and future plans. The OWG will also integrate OPSEC into all organization planning and operational processes. The OWG composition will vary depending on various projects or activities being performed. At a minimum, the OWG should include a representative from each exercise or operation, as well as any direct units associated with an exercise or operation. Recommended members include the MILDEC Officer, PSYOP Officer, Senior Intelligence Officer, PA Officer, Force Protection Officer, Information Assurance Officer, Local AFOSI Detachment and subordinate OPSEC coordinators. The OWG force protection member may be either a representative from the Wing Anti-terrorism Office (ATO) or installation Security Forces. The OWG should compliment installation anti-terrorism working groups (formerly Threat Working Groups), force protection working groups and critical infrastructure working groups.

Chapter 4

AIR FORCE SPECIAL OPERATIONS COMMAND OPSEC EDUCATION AND TRAINING

4.1. Purpose. Initial and annual OPSEC training provides AFSOC personnel (military and civilian) with general knowledge of the OPSEC process. Air Force contractors who have access to mission critical information will also receive the same training. This training ensures AFSOC personnel and supporting contractors understand their individual responsibilities, realize the positive benefits of proper OPSEC and gain a greater appreciation of how AFSOC uses OPSEC measures to minimize the exploitation of critical friendly information. Formal OPSEC training is accomplished through the 39 IOS and provides in-depth training designed to ensure proper management and execution of OPSEC programs.

4.2. OPSEC Education and Training is a Continuing Requirement. OPSEC awareness education and training must be provided to all AFSOC personnel, military, civil service and contracted individuals working within specific offices inside of AFSOC organizations (i.e., HQ AFSOC/A3, 16 SOW/SE, etc.) Additionally, all contractors who work "en mass" (i.e., construction projects, work crews, etc.) must ensure employees receive OPSEC training within 30 days of initial assignment to a contract on or around an AFSOC installation, organization or facility. The serving OPSEC PM or coordinator will provide this training. AFSOC OPSEC education and training is broken down into four sub-areas: initial, unit-specific, annual, and PMs and coordinators. OPSEC PMs and coordinators will track and document the completion of training for all military, civilian and contractor personnel. General guidelines for this education and training follow below.

4.2.1. Initial OPSEC education and training will be provided to all AFSOC personnel (as noted in paragraph 4.1.1.), within 90 days of arrival on-station. This may be provided through mass in-briefings such as new-comer's orientations, first-term airman centers or combined with the unit-specific training at the unit-level. This training will provide a brief overview of the OPSEC process, the importance of understanding the organization's critical information and the general adversary threat for the installation. Attendance of personnel's spouses and family members should be encouraged.

4.2.2. Unit-specific OPSEC education training when coupled with initial OPSEC training is the best approach to developing OPSEC awareness in all personnel within the organization. This training will be provided as part of unit in-processing for all new personnel and before individuals receive access to mission critical information. Unit-specific OPSEC training will provide assigned personnel familiarization with potential adversary threats related to the unit, critical information associated with the unit's mission, job specific OPSEC indicators and the OPSEC measures they will execute. **All personnel should provide OPSEC awareness training to their spouses and family members as well**.

4.2.3. Annual OPSEC Refresher Training. All personnel require annual OPSEC refresher training. This training should include, but not be limited to: 1) a review of the OPSEC process and terms, 2) review of the unit's CIL, 3) updated briefing on the local adversary threat, and 4) currently employed OPSEC measures to counter those threats.

4.2.4. OPSEC Education and Training Requirements for PMs and Coordinators.

4.2.4.1. Formal OPSEC Training. This level of training is required for all individuals designated as OPSEC PMs at wing-level or wing-equivalent and above, and HQ AFSOC Coordinators at the director-level. AFSOC personnel who are IO Red Team members, conduct MDVAs or formal OPSEC surveys, OPSEC Planners and IG inspections team members conducting OPSEC inspections are required to complete this training. At a minimum, the OPSEC PMs at the Wing-level or wing-equivalent and above must attend the AF OPSEC Course conducted by the 39th Information Operations Squadron at Hurlburt Field, FL within 90 days of appointment (120 days for HQ AFSOC Coordinators), or in the next available AF OPSEC course. Alternate OPSEC training can be acquired through the Interagency OPSEC Support Staff's (IOSS) DOD OPSEC Course or equivalent (see HQ AFSOC OPSEC PM for requirements); however, the Air Force course is the preferred method. OPSEC PMs must maintain general awareness of current OPSEC related events and seek continuation training at every opportunity. OPSEC PM training is unit-funded.

4.2.4.2. Informal OPSEC Training. Coordinators below wing-level are strongly encouraged to attend formal Air Force OPSEC training; however, coordinators below wing-level should seek training directly from their wing-level PM. Wing PMs should provide this training within a reasonable time of appointment or by the next available class. Coordinator's training is unit-funded.

4.2.4.3. Requests for formal OPSEC training must be forwarded through wing or wing-equivalent PMs to the HQ AFSOC OPSEC PM, who will prioritize the command's requirements and submit them to the AF OPSEC Course Registrar. Requests for IOSS courses may be made directly to the IOSS (www.ioss.gov). All OPSEC PMs will advise the HQ AFSOC OPSEC PM when training has been completed.

4.3. OPSEC Training Documentation. All OPSEC coordinators (including OPSEC PMs who conduct this training) will track initial and annual OPSEC training and report training metric results to respective wing- or wing-equivalent level OPSEC PMs for inclusion into their annual OPSEC self-assessment reports. Wing- or wing-equivalent level OPSEC PMs will forward their combined results to HQ AFSOC OPSEC PM.

Chapter 5

OPSEC ASSESSMENTS

5.1. Purpose. OPSEC assessments are accomplished to gauge the overall health of the OPSEC program, to examine actual practices and procedures and to identify new or previously undiscovered vulnerabilities. Commanders, PMs and coordinators use assessment results within the risk management process to implement protective measures and improve the OPSEC posture of the unit/activity.

5.2. Scheduling. AFSOC PMs will coordinate with their wing- or wing-equivalent commanders and units (including tenant units if you are the host unit) in scheduling assessments. Once the type of assessment and a recommended date are determined, contact the HQ AFSOC OPSEC PM for scheduling. A callout for IO Assessment will unusually take place each spring for the next FY with a forecast for three additional years.

5.3. Methods. There are several types of assessments available to OPSEC PMs or coordinators to gauge the effectiveness of their program. The nature of the assessment depends on the unit's mission criticality, availability of resources and commander guidance as illustrated in **Table 5.1.**

5.3.1. Program Self-Assessment.

5.3.1.1. AFSOC wing- or wing-equivalent PMs and coordinators will conduct annual self-assessments of their OPSEC programs. Self-assessments allow PMs to assess the health of their OPSEC program, evaluate compliance with applicable policies and to identify shortfalls and vulnerabilities.

5.3.1.2. Self-assessments are conducted using a checklist. This checklist provides AFSOC OPSEC PMs and coordinators a ready-to-use self-assessment tool in which to conduct their evaluation. **Attachment 3** contains a self-assessment checklist that can be used with little modification to suit specific unit/activity needs within AFSOC.

5.3.1.2.1. The checklist is based on the requirements set forth in AFI 10-701 and AFSOCI 10-701. While not all items may apply in all situations, none of the items listed should be removed from the checklist. AFSOC OPSEC PMs at wing- or wing-equivalent level may add items of local interest to the checklist.

5.3.1.2.2. Command and wing-level assessments (see **3.2.1.14.** and **3.2.2.1.4.**), SAVs and IG inspections (UCIs and SIIs) will follow this checklist.

5.3.2. Web Risk Assessment. See AFI 10-701 for an explanation of this assessment. Web Risk Assessments are scheduled through the annual IO Assessment callout.

5.3.3. Telecommunications Monitoring and Assessment Program (TMAP). See AFI 10-701 for an explanation of this assessment. TMAPs are scheduled through the HQ AFSOC OPSEC PM.

5.3.4. Staff Assistance Visit (SAV). See AFI 10-701 for an explanation of this assessment. SAVs for local unit coordinators are scheduled through the respective wing- or wing-equivalent OPSEC PM. Wing- or wing-equivalent SAVs are scheduled by the HQ AFSOC OPSEC PM.

5.3.5. Program Assessment. The HQ AFSOC OPSEC PM, wing and wing-equivalent PMs will accomplish a program assessment of their assigned unit's OPSEC programs using AFI 10-701, AFSOCI 10-701 and the self-assessment checklist located in **Attachment 3** biennially (every two years).

5.3.6. Survey. See AFI 10-701 for an explanation of this assessment. Surveys are coordinated through the HQ AFSOC OPSEC PM.

5.3.7. Multi-Discipline Vulnerability Assessments (MDVA). See AFI 10-701 for an explanation of this assessment. MDVAs are scheduled through the annual IO Assessment callout.

5.3.8. AFSOC Inspector General (IG) Evaluations. AFSOC OPSEC programs will be evaluated during operational readiness inspections and unit compliance inspections. Additional guidance is provided in AFSOCI 90-202, *Inspector General Operational Readiness Inspection* and AFSOCI 90-205, *AFSOC Self-Inspection Program*.

Table 5.1. OPSEC Assessment Types

Assessment Type	Purpose	Methodology	Frequency	Request Procedures	Reporting
Program Self-Assessment	-Program Health -Policy Compliance -Shortfalls	Self-Assessment by unit OPSEC PM/ Coordinator	Annual	N/A	OPSEC PM/ Coordinator reports to Unit CC and up channel to HHQ PM
Web Risk Assessment	OPSEC review of unit website	Website reviewed by 67 IOW as part of TMAP	Biennial	Unit CC requests through HQ AFSOC PM	Report to requesting CC
TMAP	ID bad COMSEC and OPSEC practices	Collect and analyze communications	Biennial	Unit CC requests through HQ AFSOC PM	Report to requesting CC
SAV	- Policy Compliance - Shortfalls - Provide Guidance	Wing OPSEC PMs assess subordinate units (if collocated), HQ AFSOC PM assess wing PMs	Annual As requested	N/A HQ AFSOC PM	Report to subordinate Unit CC and OPSEC PM or Coordinator

Assessment Type	Purpose	Methodology	Frequency	Request Procedures	Reporting
Program Assessment	- Policy Compliance - Health of Program	Wing OPSEC PMs assess subordinate units (if collocated), HQ AFSOC PM assess wing PMs	Biennial Biennial	Scheduled by the responsible PM	Report to subordinate Unit CC and OPSEC PM or Coordinator
OPSEC Survey	Assess unit OPSEC practice and procedures	Team analyzes documentation and interview personnel for: - IO Threat - Critical Information - Operational Procedures - Potential Indicators & Vulnerabilities	As required	Command Survey: Done in-house Formal Survey: Unit CC requests through HQ AFSOC PM	Out-brief and report to requesting CC
MDVA	Assess application of Influence Ops	IO Red Team simulates IO threats to identify vulnerabilities, operational impacts, & exercise threat response procedures	Every 3 years for installations with critical mission or subject to IO threats	Installation CC requests through HQ AFSOC PM	Out-brief & report to requesting CC

5.4. Assessment Reporting. Detailed results of OPSEC assessments are provided only to the requesting commander, commander of unit being assessed and the unit's OPSEC PM or coordinator. However, assessment information must be shared in a sanitized lessons learned, on a non-attribution basis, within the AFSOC OPSEC community via the AFSOC IO Office. The IO Office will provide detailed analysis and disseminate warranted information to OPSEC PMs and coordinators AFSOC-wide.

Chapter 6

AFSOC CRITICAL INFORMATION LIST

6.1. Purpose. The AFSOC Critical Information List (CIL) is a list of informational items which could reveal our intentions, capabilities, operations and activities to an adversary. This information is considered essential to the successful completion of AFSOC missions and should be treated as sensitive but unclassified information. As such, this information should be given additional protection beyond that of other unclassified information. (See **Attachment 2** for the complete CIL)

6.1.1. AFSOC critical information should not be disclosed to anyone not having the need for this information as a matter of course in completing their assigned duties.

6.1.2. The use of secure communications (STU-III/STE and SIPRNET) to discuss critical information should be your first choice of communicating this information.

6.1.3. When secure communications are not available, the use of encryption software and password encoding over unsecured communications is acceptable.

6.1.4. The use of unsecured communications should be used only as a last resort or if the need for timely transfer of the information is so critical that it outweighs the use of secure communications. (i.e., mission failure, life or death, etc.)

6.1.5. If using unsecured computer communications (NIPRNET), use attachments to transmit your information instead of the body of the e-mail. The attachment should be encrypted or password encoded before transmitting using the associated creation software (i.e., Microsoft Word, Excel, PowerPoint, or WinZip, etc.). Transfer of the password to the receiving party should be made by a different means of communication. (i.e., phone, fax, etc.)

6.1.6. Computer files and databases containing critical information should be stored in secure locations with limited access based on “need-to-know.” The use of Public Folders and “common drives” are discouraged unless proper controls such as logon and password or some other form of restricted access are put in place to protect the information.

6.1.7. All media including notes and working documents containing the types of information listed in the AFSOC CIL will be destroy by the appropriate method for that media when no longer needed. (Reference **Chapter 7**, Destruction of Sensitive But Unclassified Material.)

6.2. Direction. Every AFSOC unit down to squadron-level will develop unit-specific CILs. This effort will be lead by the OPSEC PM/coordinator and the CIL maintained in accordance with the directions in this instruction.

6.3. Organization. AFSOC critical information items are listed by functional area. The [ ] marks by each item contain the timeframe or conditions in which the information is considered to be critical. The AFSOC CIL is not intended to be all-inclusive. Information not listed, but that has the potential to cause mission impairment will also be considered critical information and should be treated and protected as such.

6.4. Contact Information. For additional information on AFSOC critical information, please contact the AFSOC OPSEC Program Manager.

Chapter 7

DESTRUCTION OF SENSITIVE BUT UNCLASSIFIED MATERIAL

7.1. Purpose. This chapter implements AFSOC policy on and requirements for the proper destruction of sensitive but unclassified material. It outlines the minimum procedures for destruction of materials containing sensitive but unclassified information as defined by **Chapter 6**, AFSOC Critical Information List (CIL). This destruction includes information contained within wing, group and unit CILs, FOR OFFICIAL USE ONLY, and Privacy Act information.

7.2. General. This policy is being implemented in an attempt to minimize the unauthorized accessibility to AFSOC sensitive but unclassified material in AFSOC organizations. (See **Chapter 8** for HQ AFSOC and AFSOF specific requirements for destruction of sensitive but unclassified paper materials.)

7.3. Guidance. All AFSOC assigned units will develop and implement a destruction of sensitive but unclassified material program. The program will provide for the destruction of sensitive but unclassified material as noted above.

7.3.1. Destruction of paper materials will be accomplished through the process of shredding (see **7.4.**) or burning (use the same requirements for burning classified materials).

7.3.2. Video tapes, voice recordings, and computer media (computer disk, ZIP disk, CD-R and RW, DVDs, flash drives, flash memory cards or sticks, hard drives internal or external, etc.) will follow established requirements for sanitization of that media or destruction at the same level as classified media. See your Client System Administrator (CSA), Information System Security Officer (ISSO), Security Manager and/or Special Security Office for additional information on the sanitization or destruction of these media types.

7.4. Requirements. At a minimum all programs will provide for the destruction of sensitive but unclassified paper products.

7.4.1. This destruction will include all white bonded paper, official and unofficial working papers/notes, and all other materials directly related to or containing operational information or information directly supporting operations whether routine (day-to-day) or currently tasked operations. (Please reference your unit’s CIL for additional information.)

7.4.2. This policy does not include items such as unclassified newspapers, magazines or other periodicals, and boxes and packing materials that must be recycled. Materials such as food wrappers and containers should be disposed of in proper waste collection containers.

7.4.3. Paper material destroyed through shredding will use “cross-cut” shredders shredding at no greater than 5/32” x 2”.

7.4.3.1. Because many units have already expended funding for strip shredders, it is permissible for units to build in an attrition schedule for replacing/upgrading their shedders to meet the requirements noted in this chapter. However, this schedule will not extend beyond the fourth quarter of FY07.

7.5. Roles and Responsibilities.

7.5.1. Commanders: Responsible for the development of their program and implementation of this policy.

7.5.2. Supervisors are responsible for adhering to and ensuring the commanders' shredding policies are followed by assigned or attached personnel.

7.5.3. Assigned personnel:

7.5.3.1. Must follow established shredding procedures.

7.5.3.2. Ensure the destruction of sensitive but unclassified materials as noted in this chapter.

7.5.4. OPSEC PMs and Coordinators: Responsible to their respective commanders for implementation and management of their program, to include any established inspection procedures used to ensure individual units are in compliance with this policy.

7.6. Shredders. For information on currently available shredders authorized for the destruction of classified and unclassified material refer to the following web site, **https://www.gsaadvantage.gov/** and enter the word "shredder" into the search window.

Chapter 8

HQ AFSOC DESTRUCTION OF SENSITIVE BUT UNCLASSIFIED MATERIAL PROGRAM

8.1. Purpose. This chapter covers the specific requirements for 100-percent destruction of sensitive but unclassified paper material for HQ AFSOC and the Air Force Special Operations Forces (AFSOF), formerly known as the WarFighting Headquarters. This program replaces HOI 31-401, *Shredding Procedures for HQ AFSOC*, dated 1 June 2002.

8.1.1. It outlines the minimum procedures for destruction of paper materials containing sensitive but unclassified information as defined by **Chapter 6**, AFSOC Critical Information List (CIL). This destruction includes information contained within command, directorate and AFSOF CILs, FOR OFFICIAL USE ONLY, and Privacy Act information.

8.2. Guidance. HQ AFSOC directorates and AFSOF will shred all white bonded paper, official and unofficial working papers/notes, and all other materials directly related to or containing operational information or information directly supporting operations whether routine (day-to-day) or currently tasked operations, ensuring all sensitive but unclassified materials are shredded and not placed into trash or recycle receptacles. (Please reference your unit's CIL for additional information.)

8.2.1. This policy does not include items such as unclassified newspapers, magazines or other periodicals, and boxes and packing materials that must be recycled. Materials such as food wrappers and containers should be disposed of in proper waste collection containers.

8.2.2. For destruction information on other sensitive but unclassified materials reference **Chapter 7** of this instruction.

8.3. Responsibilities.

8.3.1. HQ AFSOC and AFSOF directors:

8.3.1.1. Responsible for implementing the 100-percent shredding policy for their directorate.

8.3.1.2. Responsible for ensuring their personnel are aware of and follow established shredding procedures.

8.3.1.3. Ensure only authorized shredding equipment is purchased and serviceability is maintained at all times.

8.3.1.4. Incorporate shredding procedures with other security programs; for example, end-of-day security checks.

8.3.2. HQ AFSOC and AFSOF supervisors are responsible for adhering to and ensuring the directors' shredding policies are followed by assigned or attached personnel.

8.3.3. HQ AFSOC and AFSOF personnel:

8.3.3.1. Must follow established shredding procedures.

8.3.3.2. Ensure the destruction of sensitive but unclassified materials as noted in this chapter.

8.3.4. OPSEC Coordinators: Responsible to their respective directors for implementation and management of their program, to include any established inspection procedures used to ensure individual units are in compliance with this policy.

8.4. Procedures.

8.4.1. Directors will establish specific procedures to implement their shredding program. To help prevent a security violation, do not mix/store classified and unclassified material to be shredded together.

8.4.2. All materials noted in paragraph **8.2.** will be shredded as soon as practicable or when no longer needed. Documents may be shredded daily or weekly depending on amount and volume to be destroyed but should be protected from compromise until shredded.

8.4.3. At no time will any paper product or material containing sensitive but unclassified information be disposed of using the recycling or trash collection system.

8.4.4. If unclassified shredders are used they must be "cross-cut" shredders shredding at no greater than 5/32" x 2".

8.4.5. Ensure classified and unclassified shredders are clearly marked to prevent the destruction of classified material in an unclassified shredder.

8.5. Shredders. For information on currently available shredders authorized for the destruction of classified and unclassified material refer to the following web site, **https://www.gsaadvantage.gov/** and enter the word "shredder" into the search window.

Chapter 9

AFSOC OPSEC ELECTRONIC SYSTEMS SECURITY ASSESSMENTS

9.1. General. AFSOC personnel use unsecured communications systems such as telephones, cellular phones, radios, facsimile, pagers, computer networks, and other wired and wireless electronic devices to conduct day-to-day official business. Adversaries can easily monitor these unsecured systems providing themselves with valuable information on our military capabilities, limitations, intentions, and activities.

9.2. Telecommunications Monitoring and Assessment Program (TMAP). The 25th Information Operations Squadron (IOS) Electronic Systems Security Assessment (ESSA) team (proposed AFSOC ESSA Center) is the lead unit for monitoring AFSOC unsecured and unprotected communications systems. Their primary tasking is to determine if AFSOC personnel are using sound OPSEC and COMSEC practices. The information collected is analyzed to determine if any sensitive but unclassified information transmitted on unsecured and unprotected systems could adversely affect AFSOC operations.

9.2.1. The 25 IOS ESSA team conduct assessments on a continuous basis with monitoring resources adjusted to accommodate exercises, crises, contingencies, and conflicts. The monitoring and subsequent assessing of data are designed to thoroughly examine AFSOC communications systems procedures associated with a specific weapons system, operations, or activity, and document their vulnerability to an adversary's signal intelligence exploitation. Through systematic data assessment and analytical procedures, the ESSA team documents the threat, isolates existing or potential OPSEC vulnerabilities and identifies procedures to minimize or eliminate OPSEC vulnerabilities. TMAP is an integral part of the AFSOC OPSEC and IO programs with future applications in supporting both AFSOC Red Teaming and CounterIntelligence efforts. It is a very effective tool to identify real-world problems that can adversely affect our warfighting effectiveness.

9.2.2. During assessments, the ESSA team will look for such items as stereotyped patterns or administrative and physical security procedures that can routinely surface as possible sources of intelligence losses. The assessment provides commanders and directors with a product that defines, investigates, and offers specific procedures for correction of problem areas.

9.3. Telecommunications Monitoring and Assessment Program Reports. TMAP reports provide commanders, directors and operational planners with near real-time reports of sensitive but unclassified information disclosures that may adversely affect AFSOC operations. Commanders, directors and operational planners should use these reports for evaluating the effectiveness of OPSEC measures and/or developing measures to diminish the value of disclosed information. They may also use these reports to identify and focus training requirements and to justify developing and funding corrective actions.

9.4. Telecommunications Monitoring and Assessment Program Authority. HQ AIA ESSA Tasking Cell is the only AF element that can task assigned ESSA elements to monitor AF activities and organizations. Only these assigned ESSA elements (includes the 25 IOS) are authorized to conduct TMAP activities. They in turn, perform TMAP activities in a manner that satisfies the legitimate, legal needs of the Air Force to provide OPSEC while protecting the privacy, legal rights, and civil liberties of those persons whose communications are subject to TMAP monitoring.

9.5. AFSOC's Program. OPSEC and COMSEC requirements and guidance for the command's ESSA program are provided by the AFSOC/CC and executed by the HQ AFSOC OPSEC PM.

9.5.1. Responsibilities:

9.5.1.1. AFSOC Commanders and HQ Directorates will provide their unit's requirements to the HQ AFSOC OPSEC PM through their OPSEC PMs and coordinators.

9.5.1.2. AFSOC OPSEC PM:

9.5.1.2.1. Is the AFSOC POC for all TMAP operations.

9.5.1.2.2. Will collect all TMAP requests, prioritize requests and provide the command's inputs to the AIA ESSA Tasking Cell based on current and on-going mission taskings (including special access programs).

9.5.1.2.3. Manage the implementation and reporting of each tasking.

9.5.1.3. OPSEC PMs will:

9.5.1.3.1. Act as the Wing or SOG's POC for all TMAP requests or taskings.

9.5.1.3.2. Use TMAP to continuously evaluate OPSEC measures to determine specific OPSEC weaknesses, and implement and evaluate improvement actions.

9.5.1.3.3. Include TMAP assessments in appropriate operations and exercise plans.

9.5.1.3.4. Forward and coordinate all TMAP requests with the HQ AFSOC OPSEC PM.

9.5.1.3.5. Help arrange specialized communications support as needed to meet TMAP tasking requirements.

9.5.1.3.6. Restrict knowledge of the TMAP scheduled activities to those with a need-to-know.

9.5.1.3.7. Provide TMAP personnel operating instructions, security classification guides, CILs and other mission related documents required for their operations.

9.5.1.3.8. Ensure the team has access to OPSEC training documents, programs, circuit diagrams, phone numbers (including cell phones, pager, and PDAs), radio logs and frequencies, traffic records, and other needed documents.

9.5.1.4. OPSEC Coordinators will:

9.5.1.4.1. Act as the unit/directorate's POC for all TMAP requests or taskings.

9.5.1.4.2. Forward requests for TMAP assessments to their OPSEC PM (HQ Directorate will forward request directly to the AFSOC OPSEC PM).

9.5.1.4.3. Restrict knowledge of the TMAP scheduled activities to those with a need-to-know.

9.5.1.4.4. Provide operational orders and plans, operating instructions, security classification guides, and other mission related documents including OPSEC training documents, programs, circuit diagrams, phone numbers (including cell phones, pager, and PDAs), radio logs and frequencies, traffic records, and other needed documents to the OPSEC PM to support TMAP operations.

9.6. Reference. Additional information on TMAP can be found in AFI 33-219, *Telecommunications Monitoring and Assessment Program*.

Chapter 10

AFSOC OPSEC CONTRACT SECURITY REQUIREMENTS

10.1. Purpose. This chapter establishes requirements and procedures necessary to ensure contractors provide OPSEC protection for AFSOC's critical information through the completion of a DD Form 254, *DOD Contract Security Classification Specification*, for all AFSOC contracts where contracted individuals or contractors who work "en mass" (i.e., construction projects, work crews, etc.) will have access to an AFSOC installation, organization, facility or information. This requirement does not apply to individuals who infrequently access an AFSOC installation or facility (i.e., once or twice per month for an hour or two per visit).

10.1.1. Our objectives for this requirement are to:

10.1.1.1. Protect planned operational activities by preventing the inadvertent disclosure of unclassified information relating to or revealing a possible classified operation.

10.1.1.2. To preserve secrecy concerning specific scenario events and a USSOCOM or AFSOC response to these events.

10.1.1.3. To identify OPSEC vulnerabilities and recommend protective measures which will serve to enhance the security of future operations.

10.2. Guidance. The government program manager and contracting official will include the following requirements into all AFSOC contracts as noted above. A contractor shall not implement OPSEC requirements nor shall they impose any OPSEC requirements on a subcontractor without prior approval of the Air Force. Contracts as noted, will have a completed DD Form 254 attached with the following areas completed:

10.2.1. Block 11.j. *Have Operations Security (OPSEC) Requirements* will be marked as "yes."

10.2.2. Block 14. will be marked as "yes" and have the following statement:

"Ref. 11.j. The contractor and his employees will operate under HQ AFSOC *(or 16 SOW, etc.)* OPSEC procedures for the control and destruction of sensitive but unclassified information or materials containing such information, in all areas where the contractor or his employees may operate in the performance of this contract, whether contractor or government owned. See attachment no. ______ *(enter attachment number)* for additional OPSEC information." (See **Attachment 4** of this instruction for an example of the referenced attachment.)

10.3. Execution. AFSOC employed contractors will be provided unit-specific OPSEC education training by the assigned unit/directorate's OPSEC program manager/coordinator on the unit/directorate's OPSEC requirements before being given full access to or around an AFSOC installation, organization, facility or information, but not more than 30 days prior to initial access. Individual training will be developed and applied as required by the level of contact with AFSOC critical information.

10.4. Contacts. OPSEC requirements, Critical Information Lists and assistance can be found at the following:

10.4.1. For AFSOC reference AFI 10-701 or contact the HQ AFSOC OPSEC Program Manager, AFSOC/A3I at 850 884-6326, DSN 579.

10.4.2. For the 16th Special Operations Wing reference HFI 10-1101 or contact the Hurlburt Field OPSEC Program Manager, 16 SOW/IO at 850 884-4565, DSN 579.

10.5. Reference. Additional information on DD Form 254, *DOD Contract Security Classification Specification*, can be found in NISPOM, AFI 31-601 and AFI 31-601/HF Sup 1.

JAMES J. WENDLING, Colonel, USAF
Director of Operation

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Joint Pub 3-54, *Joint Doctrine for Operations Security*, January 24, 1997

AFDD 2-5, *Information Operations*, 3 February 2005

AFPD 10-20, *Air Force Defensive Counterinformation Operations*, 1 October 1998

AFI 10-701, *Operations Security*, 30 September 2005

AFMAN 37-123, (will convert to 33-363) *Management of Records*

AFI 33-129, *Web Management and Internet Use*, 3 February 2005

AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*, 23 May 2002

AFPD 90-2, *Inspector General -- The Inspection System*, 1 September 1999

Abbreviations and Acronyms

AFOSI—Air Force Office of Special Investigations

AFSOF—Air Force Special Operations Forces

CI—CounterIntelligence

CIL—Critical Information List

COMSEC—Communications Security

COMPUSEC—Computer Security

DOD—Department of Defense

EW Ops—Electronic Warfare Operations

FOIA—Freedom of Information Act

IO—Information Operation

IOSS—Interagency OPSEC Support Staff

INFOSEC—Information Security

JCS—Joints Chiefs of Staff

JP—Joint Publication

MDVA—Multi-disciplined Vulnerability Assessment

MILDEC—Military Deception

NSC—National Security Council

NSTISSI—National Security Telecommunications and Information Systems Security Instruction

NW Ops—Network Warfare Operations

OPSEC—Operations Security

OWG—OPSEC Working Group

PA—Public Affairs

PM—Program Manager

PSYOP—Psychological Operations

SII—Special Interest Item

UCI—Unit Compliance Inspection

Terms

Acquisition Program—A directed and funded effort that is designed to provide a new, improved, or continuing weapons system or automated information system capability in response to a validated operational need.

Adversary—An individual, group, organization or government that must be denied critical information. Synonymous with competitor/enemy.

Air Force Special Operations Forces (AFSOF)—(Formerly known as AFSOC War Fighting Headquarters). A headquarters focused exclusively on planning and executing military operations for AF special operations forces, leaving the principal organize, train and equip functions to the major commands above it. AFSOF encompasses the entire spectrum of conflict and Air Force special operations forces capabilities from shaping and engaging to combat operations and disengagements. AFSOF is made up of three primary elements. They consist of a command element, air operations center (AOC) and a headquarters Air Force Forces staff.

Analysis—The process by which information is examined in order to identify significant facts and/or derive conclusions.

Assessment—(1) To evaluate the worth, significance, or status of something; especially to give an expert judgment of the value or merit of something. (2) A tool for evaluating the health and effectiveness of an OPSEC program. (3) A tool for evaluating the effectiveness of OPSEC measures and involves identifying the vulnerability of operations to adversary exploitation in the light of known or estimated foreign intelligence threats.

Blog—Slang expression for a Weblog. See Weblog.

Capability—The ability to execute a specified course of action. (Joint Pub 1-02) **Note:** A capability may or may not be accompanied by an intention. When considering vulnerabilities, a capability requires the physical and mental attributes and sufficient time required for performance.

Communications Security (COMSEC)—Protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of results of such possession and study. COMSEC includes cryptosecurity, transmission security, and physical security of COMSEC materials and information.

Computer Security (COMPUSEC)—Protection resulting from all measures designed to prevent deliberate or inadvertent unauthorized disclosure, acquisition, manipulation, modification, or loss of information contained in a computer system, as well as measures designed to prevent denial of authorized use of the system.

Counterintelligence—Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign powers, organizations, persons, or international terrorist activities.

Critical Information—Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively to guarantee failure or unacceptable consequences for friendly mission accomplishment (See definition for "Sensitive Information").

Critical Information List (CIL)—Those areas, activities, functions, or other matters that a facility/ organization considers most important to keep from adversaries.

Deception—Measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce an enemy to react in a manner prejudicial to its interests.

Electronic Warfare Operations (EW OPS)—Military action involving the use of electromagnetic energy to determine, exploit, reduce, or prevent adversary use of the electromagnetic spectrum. There are three divisions within electronic warfare: electronic attack, electronic protection, and electronic warfare support.

Freedom of Information Act (FOIA)—A provision that any person has a right, enforceable in court, of access to federal agency records, except to the extent that such records (or portions thereof) are protected from disclosure by one of nine exemptions.

Indicators—Data derived from friendly detectable actions and open-source information that adversaries can interpret and piece together with other indicators to reach personal conclusions or official estimates to derive critical or sensitive information concerning friendly intentions, capabilities, or activities. Sometimes referred to as OPSEC indicators.

Information Operations (IO)—Actions taken to affect adversary information and information systems while defending one's own information and information systems. (Joint Pub 1-02)

Information Security (INFOSEC)—Result of any system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure of information, the protection of which is authorized by executive order or statute.

Military Deception (MILDEC)—Actions executed to mislead foreign decision-makers, causing them to derive and accept desired appreciation of military capabilities, intentions, operations, or other activities that evoke foreign action that contribute to the originator's objectives.

Multi-Disciplined Vulnerability Assessment (MDVA)—A systematic analytical process performed to assess an installation's application of Influence Operations and security processes to determine specific vulnerabilities. MDVAs simulate various IO threats to identify an installation's or organization's vulnerabilities (OPSEC, network, physical security, etc.), operational impacts if those vulnerabilities are exploited and exercise response procedures to the simulated threat. Identifies areas of improvement to withstand, mitigate, or deter acts of violence, terrorism, sabotage or espionage.

Operations Security (OPSEC)—A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a) identify those actions that can be observed by adversary intelligence systems; b) determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c) select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

OPSEC Advisory—Advance notice of a potential threat to OPSEC. Examples include flight paths of foreign aircraft over-flying US territory, locations of foreign naval vessels with collection capabilities, and projected commercial satellite exploitation.

OPSEC Assessment—A thorough evaluation of the effectiveness of a customer's implementation of OPSEC methodology, resources, and tools. Assessments a) are used to evaluate the effectiveness of the customer's corporate level OPSEC program and b) can be used at the program level to determine whether or not a program is a viable candidate for an OPSEC survey.

OPSEC Coordinator—Normally below the wing and wing equivalent level, but also includes HQ AFSOC Directorates. Acts as an interface to direct and manage all relevant OPSEC matters. Reports to OPSEC Program Manager.

OPSEC Indicators—Data derived from friendly detectable actions/activities and open-source information that adversaries can interpret and piece together with other indicators to reach personal conclusions or official estimates to derive critical or sensitive information concerning friendly intentions, capabilities, or activities. Sometimes referred to just as indicators.

OPSEC Measure—Anything which effectively negates or mitigates an adversary's ability to exploit vulnerabilities.

OPSEC Process—An analytical process that involves five components: a) identification of critical information, b) analysis of threats, c) analysis of vulnerabilities, d) assessment of risks, and e) application of appropriate OPSEC measures (NSC 1988).

OPSEC Program—An OPSEC program is the vehicle by which the principles and practices of OPSEC are employed within an organization.

OPSEC Program Manager—At the wing and wing equivalent and above level. Focal point for OPSEC related matters and ensures OPSEC requirements are in compliance as directed from Higher Headquarters. Reviews operations plans to ensure a statement of OPSEC considerations and appropriate guidance regarding critical information are included.

OPSEC Survey—The application of OPSEC methodology at the program level. It is a detailed analysis of all activities associated with a specific operation, project or program in order to determine what exploitable evidence of classified or sensitive activity could be acquired in light of the known collection capabilities of potential adversaries.

OPSEC Vulnerability—Condition in which friendly actions provide OPSEC indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision-making.

OPSEC Working Group (OWG)—A (normally formally) designated body representing a broad range of line and staff activities within an organization that provides OPSEC advice and support to leadership and all elements of the organization.

Personnel Security—Policies and procedures to ensure granting security clearances in the best interest of national security.

Physical Security—That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, facilities, material, and documents; and to safeguard them against espionage, sabotage, damage and theft.

Psychological Operations (PSYOP)—Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals.

Risk—A measure of the potential degree to which protected information is subject to loss through adversary exploitation.

Risk Assessment—An OPSEC process of evaluating the risks of information loss based on an analysis of threats to, and vulnerabilities of, a system, operation or activity.

Risk Management—A continuous process designed to detect, assess, and control risk while enhancing performance and maximizing capabilities. Provides the basic structure for the detection, assessment, and ultimate sustained control of risk while enhancing performance and maximizing capabilities.

Sensitive But Unclassified Information—See definition for "Sensitive Information."

Sensitive Information—Information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy (NSTISSI 1997)

Special Access Program—A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level (NSC EO 1995).

Threat—The capability of an adversary coupled with his intentions to undertake any actions detrimental to the success of program activities or operations.

Threat Analysis—An OPSEC process, which examines an adversary's technical and operational capabilities, motivation, and intentions, designed to detect and exploit vulnerabilities.

Threat Assessment—An evaluation of the intelligence collection threat to a program activity, system, or operation.

Vulnerability—A condition in which friendly actions provide OPSEC indicators that may be obtained and accurately evaluated by an adversary in time to prove a basis for effective adversary decision making.

Vulnerability Analysis—In information operations, a systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. See also information operations; information system; security; vulnerability.

Vulnerability Assessment—An evaluation (assessment) to determine the vulnerability of an installation's application of Influence Operations and security processes to determine specific vulnerabilities. Identifies areas of improvement to withstand, mitigate, or deter acts of violence, terrorism, sabotage or espionage.

Weblog—(Also referred to as a “blog.”) This is a publicly accessible personal journal for an individual similar to a personal diary, but shared over the Internet. The activity of updating a blog is "blogging" and someone who keeps a blog is a "blogger." Blogs are typically updated daily using software that allows people with little or no technical background to update and maintain the blog. Postings on a blog are almost always arranged in chronological order with the most recent additions featured most prominently.

Attachment 2

AFSOC CRITICAL INFORMATION LIST (CIL)

AFSOC critical information items are listed by functional area. The [ ] marks by each item contain the timeframe or conditions in which the information is considered to be critical. The AFSOC CIL is not intended to be all-inclusive. Information not listed, but that has the potential to cause mission impairment will also be considered critical information and should be treated and protected as such.

For additional information on AFSOC critical information, please contact the HQ AFSOC OPSEC Program Manager.

1. GENERAL - Details or information related to:

   a. Units assigned, their missions and composition, Status of Resources and Training System (SORTS) status, and their association with their customers/users [Continuous]

   b. Activation or alert of any Wing or associated Reserve or Guard units [Duration]

   c. Command or Wing strategic plans and associated metrics and indicators [Until no longer current or valid]

   d. Commander and senior staff identities and composition to include: itineraries, health, leave schedules, personal affairs, and tactical behavior [Continuous]

   e. Inter-command and intra-command communications infrastructure to include: all associated entry means, encryption, encoding, authenticators (passwords), and communication procedures and discipline [Until no longer current or valid]

   f. Operating Instructions (OIs), Technical Orders (TOs), designated For Official Use Only (FOUO) information and Privacy Act information [Continuous]

   g. Security procedures to include, but not limited to Operational, Information, Industrial, Personnel, Physical, Communication, and Computer Security (Critical Information Lists) [Continuous]

      (1) Security violations and corrective actions [Until no longer current or valid]

2. OPERATIONS - Details or information related to:

   a. Operations, deployments and exercises:

      (1) Daily and deployed operations to include: mission planning, mission limitations (weather criteria, etc.) composition, and disposition; unit movements (aircraft, personnel and equipment involved), dates and locations [Until no longer current or valid]

      (2) Deployment activities to include: force planning, composition, disposition, and prepositioning including associated unit movements (aircraft, personnel and equipment involved), dates and locations [Duration of deployment or until no longer current or valid]

      (3) Training activities and purposes (exercises) to include: force planning, composition, disposition, and prepositioning including associated unit movements (aircraft, personnel and

equipment involved), dates and locations [Duration of exercise or until no longer current or valid]

(4) Summaries or details of OPLANS/CONPLANS, scenarios or objectives [Until no longer current or valid]

(5) General operations, deployment and exercise information:

(a) Actions, information or material providing insight into current operations and associated problems [Until no longer current or valid]

(b) C2 arrangements, procedures and actions necessary to control and plan operations and daily activities [Until no longer current or valid]

(c) Mission designators, call signs, abbreviations, acronyms, code words, and nicknames [Until no longer current or valid]

(d) Associated intelligence activities, capabilities, requirements, sources, and information collected; threat analysis and assumptions [Continuous]

b. Weapon system reliability, vulnerabilities or operational capabilities; requirements and limitations (current, under development or future) [Continuous]

(1) Specialized mission aircraft [Until no longer current or valid]

c. Tactics, Techniques and Procedures (TTPs) including implementation and execution procedures and associated limiting factors [Until no longer current or valid]

3. LOGISTICS - Details or information related to:

a. Aircraft or support equipment status, reliability, limitations, trends or numbers [Until no longer current or valid]

b. Maintenance schedules (overdue or scheduled maintenance, aircraft or equipment priorities, PMC/NMC status) [Until no longer current or valid]

c. Ongoing, planned and future modifications to aircraft and supporting equipment [Until no longer current or valid]

d. Types and numbers of support equipment procured for units including specialized equipment [Until no longer current or valid]

4. MISSION SUPPORT - Details or information related to:

a. Current stocks, availability and storage capacities of aircraft and support equipment parts, fuels and lubricants (inventory, requirements, special types, etc.) [Continuous]

b. Resource shortfalls (ammunition, expendables, etc.) and limiting factors (LIMFACs) [Until no longer current or valid]

c. Status of personal issue equipment (chemical, survival, and support) [Until no longer current or valid]

d. Cargo and personnel movement to include: Classification; identification codes; number of pieces; origin and destination; weight and cubic feet; commercial transport use; movement assembly areas; specialized equipment needed or used; schedules; convoy assembly; travel reservations; passenger manifests [Until no longer current or valid]

e. Infrastructure capabilities, limitations, and vulnerabilities (water, electricity, heating, etc.) [Continuous]

f. Contract types, vendors, and specifications [Until no longer current or valid]

g. Mission and operational environmental impacts [Until no longer current or valid]

h. Firefighting, security forces, and disaster preparedness capabilities, response procedures and schedules, types and numbers of support equipment and armament [Continuous]

i. Runway usage, layout, and ramp usage (taxi procedures, parking, etc.) [Continuous]

j. Trash disposal and recycle program schedules and procedures [Continuous]

k. New construction or structure modifications [Until no longer current or valid]

l. Security classification guides and security clearance requirements [Continuous]

m. Local fire department and law enforcement coordination and agreements [Until no longer current or valid]

5. MEDICAL - Details or information related to:

a. Force health assessments [Continuous]

b. Immunization status and availability [Continuous]

c. Shortfalls, limitations and restrictions of medical supplies and Medical War Reserve Material [Until no longer current or valid]

d. Request and disclosure of Medical Intelligence [Until no longer current or valid]

e. Requests for Medical Specialties in support of mission requirements [Until no longer current or valid]

6. PERSONNEL/ADMIN - Details or information related to:

a. DVs (VIPs) visits: purpose for and itineraries [Until no longer current or valid]

b. Memorandums of Agreement [Until no longer current or valid]

c. Unit manning levels (manpower strength and shortages, projections, AFSC requirements) [Until no longer current or valid]

d. Training status to include: Aircrew and ground crew proficiency, experience levels, qualifications, current and overdue requirements [Until no longer current or valid]

e. Information revealing personnel movement (orders, etc.) [Until no longer current or valid]

f. Personnel and immunization records [Continuous]

g. Duty and leave schedules [Until no longer current or valid]

h. Mobility processing (ongoing, procedures, and schedules) [Until no longer current or valid]

i. Recalls (ongoing, procedures, and codes) [Until no longer current or valid]

j. Unit Morale [Continuous]

k. Operating budgets including budget allocations (where and on what, money is being applied), unfunded requirements and POM inputs [Continuous]

Attachment 3

SELF-ASSESSMENT CHECKLIST

OPERATIONS SECURITY (OPSEC) SELF-ASSESSMENT CHECKLIST				
TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA **OPERATIONS SECURITY**	**OPR**	**DATE**		
NO.	**ITEM** ***(All references are to AFI 10-701 unless otherwise stated)***	**YES**	**NO**	**N/A**
1.	**Administrative Requirements**			
1.1.	Has the commander (all levels):			
1.1.1.	Appointed an OPSEC Program Manager (PM) or coordinator and alternate in writing (This includes the appointment of coordinators in HQ directorates)? *AFI 10-701, Para 3.1.1., 3.2. and 3.3.; AFSOCI 10-701, Para* ***2.2.1.1.2.****,* ***2.2.2.1.2.*** *and* ***2.2.2.2.2.***			
1.1.2.	Ensured the OPSEC PM or coordinator has a security clearance appropriate to the mission and function of the organization, but not lower than Secret? *AFI 10-701, Para 3.2. and 3.3.; AFSOCI 10-701, Para* ***3.2.*** *and* ***3.3.***			
1.1.3.	Ensured the OPSEC PMs and coordinators (including HQ directorates) have access to and established a NIPRNET personal and/or organizational account? *AFI 10-701, Para 3.2.; AFSOCI 10-701, Para* ***3.2.*** *and* ***3.3.***			
1.1.4.	Ensured the OPSEC PMs and HQ directorate coordinators have access to and established a SIPRNET personal and/or organizational account? *AFI 10-701, Para 3.2.; AFSOCI 10-701, Para* ***3.2.*** *and* ***3.3.***			
1.2.	OPSEC PM and/or Coordinator (includes HQ directorates):			
1.2.1.	Does the appointee reside in the operations or plans element of the organization or report directly to the organization's commander? *AFI 10-701, Para 3.1.2.; AFSOCI 10-701, Para* ***3.1.2.***			
1.2.2.	Has his/her identity (appointment letter) been forwarded to the higher headquarters (HHQ) OPSEC PM? *AFI 10-701, Para 3.2. and 3.3.; AFSOCI 10-701, Para* ***3.2.****,* ***3.3.****,* ***3.3.1.5.*** *and* ***3.3.2.5.***			

OPERATIONS SECURITY (OPSEC) SELF-ASSESSMENT CHECKLIST				
TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA **OPERATIONS SECURITY**	**OPR**	**DATE**		
NO.	**ITEM** ***(All references are to AFI 10-701 unless otherwise stated)***	**YES**	**NO**	**N/A**
1.2.3.	Is the OPSEC PM/coordinator aware of their responsibilities? *AFI 10-701, Para 3.2.1. and 3.3.1.; AFSOCI 10-701, Para **3.2.2.**, **3.3.1.** and **3.3.2.***			
2.	**OPSEC Execution Requirements**			
2.1.	Has the commander (all levels):			
2.1.1.	Developed an OPSEC program IAW HHQ policy and guidance? *AFI 10-701, Para 2.2.2.; AFSOCI 10-701, **Chapter 2**.*			
2.1.2.	Ensured his/her organization(s) has/have integrated OPSEC within day-to-day operations? *AFI 10-701, Para 2.2.2.2. and 3.1.1.; AFSOCI 10-701, Para **2.2.1.1.3.**, **2.2.2.1.3.**, **2.2.2.2.3.** and **3.1.1.***			
2.1.3.	Made OPSEC risk management decisions? *AFI 10-701, Para 3.1.1.; AFSOCI 10-701, Para **2.2.1.1.**, **2.2.2.1.**, **2.2.2.2.**, and **3.1.1.***			
2.1.4.	Directed the overall implementation of OPSEC measures? *AFI 10-701, Para 3.1.1.; AFSOCI 10-701, Para **2.2.1.1.**, **2.2.2.1.**, **2.2.2.2.** and **3.1.1.***			
2.1.5.	Ensured OPSEC is integrated with other IO activities and efforts? *AFI 10-701, Para 3.1.3.1. and 3.1.4.; AFSOCI 10-701, Para **2.2.1.1.3.**, **2.2.2.1.3.** and **2.2.2.2.3.***			
2.2.	Has the OPSEC PM (wing-level or equivalent):			
2.2.1.	Developed, coordinated and managed the OPSEC program, AFSOC OPSEC Plan and implementation of OPSEC into day-to-day operations throughout the wing? *AFI 10-701, Para 3.2.1.1.; AFSOCI 10-701, Para **3.2.2.1.***			
2.2.1.1.	Posted OPSEC multimedia aids throughout Wing facilities? *AFSOCI 10-701, Para **3.2.2.1.1.***			
2.2.1.2.	Ensured primary and alternate OPSEC coordinators have been selected for each group and squadron and their pictures and phone numbers are posted throughout their assigned facilities? *AFSOCI 10-701, Para **3.2.2.1.2.***			

OPERATIONS SECURITY (OPSEC)
SELF-ASSESSMENT CHECKLIST

TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA	OPR	DATE
OPERATIONS SECURITY		

NO.	ITEM *(All references are to AFI 10-701 unless otherwise stated)*	YES	NO	N/A
2.2.1.3.	Ensured each unit developed a unit specific CIL and posted a copy at each work station? *AFSOCI 10-701, Para **3.2.2.1.3.***			
2.2.1.4.	Conducted annual OPSEC inspections of respective assigned organization's OPSEC program as required? *AFSOCI 10-701, Para **3.2.2.1.4.***			
2.2.2.	Acted as primary advisor to the commander on all OPSEC matters? *AFSOCI 10-701, Para **3.2.2.2.***			
2.2.3.	Incorporated OPSEC into wing plans, exercises, activities and wing-to-tenant/local community agreements? *AFI 10-701, Para 3.1.3. and 3.2.1.2.; AFSOCI 10-701, Para **3.2.2.5.***			
2.2.4.	Incorporated OPSEC lessons learned from wing/group and unit operations and exercises as well as other operations and exercises into the wing's planning process and forwarded lessons learned to appropriate depositories? *AFI 10-701, Para 3.2.1.3.; AFSOCI 10-701, Para **3.2.2.6.***			
2.2.5.	Developed and implemented the commander's OPSEC policies and wing's CIL? *AFI 10-701, Para 3.2.1.4.; AFSOCI 10-701, Para **3.2.2.3.***			
2.2.6	Developed, issued and implemented policies, supplements or other directions as required? *AFSOCI 10-701, Para **3.2.2.7.***			
2.2.7.	Developed and maintained an effective working relationship with Intelligence and OSI CounterIntelligence and requested additional intelligence and counterintelligence support to meet their OPSEC program requirements? *AFSOCI 10-701, Para **3.2.2.9.***			
2.2.8.	Reviewed the wing's CIL during January of each year and forwarded the new/updated CIL to the HQ AFSOC OPSEC PM by 31 January of each year? *AFSOCI 10-701, Para **3.2.2.3.***			
2.2.9.	Developed procedures to ensure wing critical information, OPSEC indicators and sensitive activities are identified and controlled? *AFI 10-701, Para 3.2.1.5.; AFSOCI 10-701, Para **3.2.2.4.***			

OPERATIONS SECURITY (OPSEC) SELF-ASSESSMENT CHECKLIST				
TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA **OPERATIONS SECURITY**		**OPR**	**DATE**	
NO.	**ITEM** ***(All references are to AFI 10-701 unless otherwise stated)***	**YES**	**NO**	**N/A**
2.2.10.	Ensured OPSEC reviews are conducted on all wing web pages prior to the information being placed, updated, or modified on the web page and annually thereafter? *AFI 10-701, Para 3.2.1.6.; AFSOCI 10-701, Para **3.2.2.11.**; and AFI 33-129*			
2.2.11.	Ensured OPSEC considerations are included in PA's review and approval process for the publishing and/or releasing of information to or that may be viewed by the public? *AFI 10-701, Para 3.2.1.7.; AFSOCI 10-701, Para **3.2.2.10.***			
2.2.12.	Ensured OPSEC is integrated with other Information Operations (IO) and Influence Operations activities and efforts? *AFI 10-701, Para 3.2.1.9.; AFSOCI 10-701, Para **3.2.2.12.***			
2.2.13.	Formed and chaired the OPSEC working group (normally wing-level) consisting of appropriate IO and security disciplines and applicable supporting organizations? *AFI 10-701, Para 3.2.1.12. and 3.5.; AFSOCI 10-701, Para **3.2.2.14.** and **3.5.***			
2.13.1.	Solicited, published, and distributed agenda items one week prior to each meeting? *AFSOCI 10-701, Para **3.2.2.14.1.***			
2.13.2.	Recorded, published, and distributed minutes NLT two weeks after the meeting; sending a copy of these minutes to the HQ AFSOC OPSEC PM? *AFSOCI 10-701, Para **3.2.2.14.2.***			
2.13.3.	Forwarded OPSEC working group recommendations to the appropriate commander for review and approval? *AFSOCI 10-701, Para **3.2.2.14.3.***			
2.2.14.	Participated in all applicable working groups? *AFSOCI 10-701, Para **3.2.2.15.***			
2.2.15.	Worked with the local contracting office to ensure all appropriate contractual documents (i.e., Statements of Work (SOW), Requests for Proposals (RFP) and similar documentation) are evaluated for specific statements or requirements that address security criteria for protecting OPSEC critical information and OPSEC indicators? *AFI 10-701, Para 3.1.3. and 3.2.1.15.; AFSOCI 10-701, Para **3.2.2.17.***			

OPERATIONS SECURITY (OPSEC)
SELF-ASSESSMENT CHECKLIST

TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA **OPERATIONS SECURITY**	OPR	DATE

NO.	ITEM *(All references are to AFI 10-701 unless otherwise stated)*	YES	NO	N/A
2.2.16.	Ensured OPSEC considerations are integrated into the acquisition cycle? *AFI 10-701, Para and 3.2.1.15.; AFSOCI 10-701, Para* ***3.2.2.17.***			
2.2.17.	Served as the wing focal point for managing and scheduling all ESSA requirements? *AFI 10-701, Para 3.2.1.17.; AFSOCI 10-701, Para* ***3.2.2.19.*** *and AFI 33-219*			
2.2.18.	Coordinated their OPSEC program (host unit) with tenant unit OPSEC PMs and/or coordinators? *AFI 10-701, Para 3.2.; AFSOCI 10-701, Para* ***3.2.***			
2.2.19.	Submitted an annual budget requirement to the HQ AFSOC OPSEC PM for inclusion into the AFSOC budget process? *AFSOCI 10-701, Para* ***3.2.2.21.***			
2.2.20.	Established and maintained a wing OPSEC continuity binder IAW the AFSOC OPSEC Plan? *AFSOCI 10-701, Para* ***3.2.2.22.***			
2.2.21.	(Tenant unit OPSEC PMs) Coordinated and integrated with host wing OPSEC initiatives? *AFI 10-701, Para 3.2.; AFSOCI 10-701, Para* ***3.2.***			
2.2.22.	(Tenant unit OPSEC PMs) Participated in host wing's OPSEC working group? *AFI 10-701, Para 3.2.; AFSOCI 10-701, Para* ***3.2.***			
2.3.	Has the OPSEC Coordinator (below wing-level or within HQ directorates):			
2.3.1.	Implemented and executed OPSEC into day-to-day operations utilizing commander/directorate and HHQ OPSEC PM policy and guidance throughout the organization? *AFI 10-701, Para 3.3.1.1.; AFSOCI 10-701, Para* ***3.3.1.1.***, ***3.3.1.1.1.*** *and* ***3.3.1.1.2.***			
2.3.1.1.	Posted OPSEC multimedia aids throughout the unit? *AFSOCI 10-701, Para* ***3.3.2.1.1.***			
2.3.1.2.	Posted their picture and phone number throughout assigned facilities? *AFSOCI 10-701, Para* ***3.3.2.1.2.***			

OPERATIONS SECURITY (OPSEC)
SELF-ASSESSMENT CHECKLIST

TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA	OPR	DATE
OPERATIONS SECURITY		

NO.	ITEM *(All references are to AFI 10-701 unless otherwise stated)*	YES	NO	N/A
2.3.1.3.	Developed a unit/directorate specific CIL and posted a copy at each work station? *AFSOCI 10-701, Para **3.3.1.1.3.** and **3.3.2.1.3.***			
2.3.2.	Acted as primary advisor to the commander on all OPSEC matters? *AFSOCI 10-701, Para **3.3.1.2.** and **3.3.2.2.***			
2.3.3.	Incorporated OPSEC into organizational plans, exercises and activities? *AFI 10-701, Para 3.1.3. and 3.3.1.2.; AFSOCI 10-701, Para **3.3.1.6.** and **3.3.2.6.***			
2.3.4.	Incorporated OPSEC lessons learned from unit/directorate operations and exercises as well as other operations and exercises into the unit/ director's planning process? *AFSOCI 10-701, Para **3.3.1.7.** and **3.3.2.7.***			
2.3.5.	Developed and implemented the commander's/directorate's OPSEC policy and CIL? *AFI 10-701, Para 3.3.1.4.; AFSOCI 10-701, Para **3.3.1.3.** and **3.3.2.3.***			
2.3.6.	Reviewed the unit/directorate's CIL during January of each year and forward the new/updated list to the wing OPSEC PM (HQ AFSOC OPSEC PM for directorates) by 31 Jan of each year? *AFSOCI 10-701, Para **3.3.1.3.** and **3.3.2.3.***			
2.3.7.	Developed procedures to ensure critical information, OPSEC indicators and sensitive activities are identified and controlled? *AFI 10-701, Para 3.3.1.5.; AFSOCI 10-701, Para **3.3.1.4.** and **3.3.2.4.***			
2.3.8.	Implemented policies, supplements or other directions as required? *AFSOCI 10-701, Para **3.3.1.8.** and **3.3.2.8.***			
2.3.9.	Conducted OPSEC reviews on unit/directorate web pages annually and prior to information being placed, updated, or modified on the web page? *AFI 10-701, Para 3.3.1.6.; AFSOCI 10-701, Para **3.3.1.11.** and **3.3.2.11.***			
2.3.10.	Ensured OPSEC reviews are conducted on unit/directorate information to be published or released to or that may be viewed by the public? *AFI 10-701, Para 3.3.1.7.; AFSOCI 10-701, Para **3.3.1.10.** and **3.3.2.10.***			

OPERATIONS SECURITY (OPSEC) SELF-ASSESSMENT CHECKLIST				
TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA **OPERATIONS SECURITY**		**OPR**	**DATE**	
NO.	**ITEM** ***(All references are to AFI 10-701 unless otherwise stated)***	**YES**	**NO**	**N/A**
2.3.11.	Participated in all applicable working groups as required? *AFI 10-701, Para 3.3.1.10. and 3.5.; AFSOCI 10-701, Para* ***3.3.1.13.*** *and* ***3.3.2.13.***			
2.3.12.	Utilized assessment results to correct/resolve/mitigate discovered vulnerabilities and aid organization OPSEC awareness efforts? *AFI 10-701, Para 3.3.1.11.; AFSOCI 10-701, Para* ***3.3.1.17.*** *and* ***3.3.2.17.***			
2.3.13.	Integrated OPSEC into all acquisition programs and contractor support documents? *AFI 10-701, Para 3.1.3. and 3.3.1.13.; AFSOCI 10-701, Para* ***3.3.1.15.*** *and* ***3.3.2.15.***			
2.3.14.	Coordinated with appropriate organizations and wing/wing-equivalent senior leadership to resolve/mitigate Web Risk Assessment, TMAP, MDVA and other OPSEC assessment findings as required? *AFI 10-701, Para 3.3.1.14.; AFSOCI 10-701, Para* ***3.3.1.17.*** *and* ***3.3.2.17.***			
2.3.15.	Served as the unit/directorate focal point for TMAP operations? *AFI 10-701, Para 3.3.1.15.; AFSOCI 10-701, Para* ***3.3.1.16.****,* ***3.3.2.16.****, and AFI 33-219*			
2.3.16.	Submitted an annual budget requirement (directorates only) to the HQ AFSOC OPSEC PM for inclusion into the AFSOC budget process? *AFSOCI 10-701, Para* ***3.3.1.18.***			
2.3.17.	Established and maintained a unit/directorate OPSEC continuity binder IAW the AFSOC OPSEC Plan? *AFSOCI 10-701, Para* ***3.3.1.19.*** *and* ***3.3.2.18.***			
2.3.18.	(Tenant unit OPSEC coordinators) Closely coordinated and integrated their programs with host wing OPSEC initiatives? *AFI 10-701, Para 3.2. and 3.3.; AFSOCI 10-701, Para* ***3.3.***			
2.3.19.	(Tenant unit OPSEC coordinators) Participated in host wing's OPSEC working groups? *AFI 10-701, Para 3.2. and 3.3.; AFSOCI 10-701, Para* ***3.3.***			
3.	**Training Requirements**			
3.1.	Has the OPSEC PM (wing-level or equivalent):			

OPERATIONS SECURITY (OPSEC)
SELF-ASSESSMENT CHECKLIST

TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA	OPR	DATE
OPERATIONS SECURITY		

NO.	ITEM *(All references are to AFI 10-701 unless otherwise stated)*	YES	NO	N/A
3.1.1.	Attended OPSEC PM training within 90 days of their appointment or been scheduled for the next available Air Force OPSEC PM course? *AFI 10-701, Para 4.1.2.2.; AFSOCI 10-701, Para* ***3.2.2.8.*** *and 4.1.1.4.1.*			
3.1.2.	Ensured OPSEC training for coordinators below wing level is accomplished within a reasonable time of appointment or by the next available class? *AFI 10-701, Para 4.1.2.2.; AFSOCI 10-701, Para 4.1.1.4.2.*			
3.1.3.	Maintained a general awareness of current OPSEC related events and sought continuation training at every opportunity? *AFI 10-701, Para 4.1.2.2.; AFSOCI 10-701, Para 4.1.1.4.1.*			
3.1.4.	Ensured all OPSEC Planners, IO Red Team members and personnel performing OPSEC surveys and IG inspections are provided OPSEC training? *AFI 10-701, Para 4.1.2.1.; AFSOCI 10-701, Para 4.1.1.4.1.*			
3.1.5.	Provided management, development and oversight of appropriate OPSEC training and conducted training as required? *AFI 10-701, Para 3.2.1.10. and 4.1.1.2.; AFSOCI 10-701, Para* ***3.2.2.8.*** *and 4.1.1.*			
3.1.5.1.	Ensured all wing personnel receive initial (within 90 days of arrival at duty station) and annual OPSEC training and maintain documentation of personnel trained for both initial and annual training? *AFSOCI 10-701, Para* ***3.2.2.8.1.*** *and 4.1.1.1.*			
3.1.6.	Coordinated with other wing security PMs (e.g., COMSEC, COMPUSEC, Force Protection, INFOSEC, and Personnel Security) to incorporate OPSEC concepts and lessons learned into their security training sessions? *AFSOCI 10-701, Para* ***3.2.2.8.2.***			
3.2.	Has the OPSEC coordinator (below wing-level or within HQ directorates):			
3.2.1.	Conducted/Attended OPSEC training as required? *AFSOCI 10-701, Para* ***3.3.1.9.*** *and* ***3.3.2.9.***			

OPERATIONS SECURITY (OPSEC)
SELF-ASSESSMENT CHECKLIST

TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA	OPR	DATE
OPERATIONS SECURITY		

NO.	ITEM *(All references are to AFI 10-701 unless otherwise stated)*	YES	NO	N/A
3.2.1.1.	Provided management and conducted unit-specific and annual OPSEC training upon arrival of newly assigned personnel (military, civilian and contractors) and recurring training annually thereafter? *AFI 10-701, Para 3.3.1.8. and 4.1.1.1.; AFSOCI 10-701, Para* ***3.3.1.9.1.****,* ***3.3.2.9.1.****, 4.1.1.2. and 4.1.1.3.*			
3.2.1.2.	Ensured OPSEC training, unit-specific and annual recurring training provide, as a minimum familiarization with the OPSEC process, potential adversary threats related to the unit, critical information associated with the unit's mission, job specific OPSEC indicators and the OPSEC measures they will execute? *AFI 10-701, Para 4.1.1.2.; AFSOCI 10-701, Para 4.1.1.2. and 4.1.1.3.*			
3.2.2.3.	(Unit coordinators) Been scheduled for OPSEC training within a reasonable time of appointment or by the next available class? *AFI 10-701, Para 4.1.2.2.; AFSOCI 10-701, Para* ***3.3.2.9.2.*** *and 4.1.1.4.2.*			
3.2.2.4.	(Directorate coordinators) Attended OPSEC PM training within 120 days of their appointment or been scheduled for the next available Air Force OPSEC PM course? *AFI 10-701, Para 4.1.2.2.; AFSOCI 10-701, Para* ***3.3.1.9.2.*** *and 4.1.1.4.1.*			
3.2.2.5.	Tracked and documented training for all military, civilian and contractor personnel? *AFI 10-701, Para 4.1.1. and 4.1.1.3.; AFSOCI 10-701, Para* ***3.3.1.9.1.****,* ***3.3.2.9.1.*** *and 4.1.2.*			
4.	**OPSEC Assessment Requirements**			
4.1.	Has the OPSEC PM (wing-level or equivalent):			
4.1.1.	Ensured OPSEC reviews considered the proliferation of internet/web-based bulletin boards and logs (blogs) and evaluated the risk presented by web content in annual OPSEC assessments? *AFI 10-701, Para 3.2.1.8.; AFSOCI 10-701, Para* ***3.2.2.11.1.***			
4.1.2.	Coordinated and facilitated OPSEC assessments IAW AFI 10-701, Chapter 5? *AFI 10-701, Para 3.2.1.11., 3.2.1.13. and Chapter 5, Table 2, OPSEC Assessment Types; AFSOCI 10-701, Para* ***3.2.2.13.*** *and* ***3.2.2.20.***			

OPERATIONS SECURITY (OPSEC) SELF-ASSESSMENT CHECKLIST				
TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA OPERATIONS SECURITY	**OPR**	**DATE**		
NO.	**ITEM** ***(All references are to AFI 10-701 unless otherwise stated)***	**YES**	**NO**	**N/A**
4.1.3.	Officially requested or had a web risk assessment conducted as part of a survey, an MDVA, or a stand-alone assessment at least biennially? *AFI 10-701, Para 5.3.2. and Chapter 5, Table 2, OPSEC Assessment Types; AFSOCI 10-701, Para* ***3.2.2.20.***			
4.1.4.	Conducted or had an outside agency conduct a survey? *AFI 10-701, Para 5.3.5. and Chapter 5, Table 2, OPSEC Assessment Types; AFSOCI 10-701, Para* ***3.2.2.20.***			
4.1.5.	Officially requested, for the commander, an MDVA if one has not been conducted in three years? *AFI 10-701, Para 5.3.6. and Chapter 5, Table 2, OPSEC Assessment Types*			
4.1.6.	Conducted annual Staff Assistance Visits (SAVs) to all subordinate units as required? *AFI 10-701, Para 3.2.1.16., 5.3.4. and Chapter 5, Table 2, OPSEC Assessment Types; AFSOCI 10-701, Para* ***3.2.2.18.***			
4.2.	Has the OPSEC PM and/or Coordinator (including HQ directorates):			
4.2.1.	Conducted annual OPSEC self-assessments as appropriate IAW Chapter 5, AFI 10-701? *AFI 10-701, Para 3.1.5., 3.3.1.9., 5.3.1. and Chapter 5, Table 2, OPSEC Assessment Types; AFSOCI 10-701, Para* ***3.2.2.13.****,* ***3.3.1.12.****,* ***3.3.2.12.*** *and* ***5.3.1.***			
4.2.2.	Officially requested or had a telecommunications monitor conducted as part of a survey, an MDVA, or a stand-alone assessment at least biennially? *AFI 10-701, Para 5.3.3. and Chapter 5, Table 2, OPSEC Assessment Types; AFSOCI 10-701, Para* ***3.2.2.20.****,* ***3.3.1.16.*** *and* ***3.3.2.16.***			
5.	**OPSEC Reporting Requirements**			
5.1.	Has the OPSEC PM (wing-level or equivalent):			
5.1.1.	Reported annual OPSEC self-assessments findings to HQ AFSOC OPSEC PM NLT 15 October of each year? *AFI 10-701, Para 3.2.1.11., 3.3.1.9. and Chapter 5, Table 2, OPSEC Assessment Types; AFSOCI 10-701, Para* ***3.2.2.13.***			
5.1.2.	Forwarded self-assessment findings containing:			

OPERATIONS SECURITY (OPSEC)
SELF-ASSESSMENT CHECKLIST

TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA **OPERATIONS SECURITY**	OPR	DATE

NO.	ITEM *(All references are to AFI 10-701 unless otherwise stated)*	YES	NO	N/A
5.1.2.1.	Training metrics for all subordinate units. *AFI 10-701, Para 2.2.2.14. and 4.1.1.3.; AFSOCI 10-701, Para* ***3.2.1.15.***			
5.1.2.2.	Number of vulnerability reports forwarded to the IO Threat Analysis Center. *AFI 10-701, Para 2. 2.2.14.; AFSOCI 10-701, Para* ***3.2.1.15.***			
5.1.2.3.	Number and type of survey/assessment received by subordinate units (command survey, TMAP, MDVA, Web Risk Assessments, etc.), *AFI 10-701, Para 2.2.2.14.; AFSOCI 10-701, Para* ***3.2.1.15.***, and			
5.1.2.4.	Any other information deemed of OPSEC importance. *AFI 10-701, Para 2.2.2.14., 3.2.1.11. and 3.3.1.9.; AFSOCI 10-701, Para* ***3.2.1.15.***			
5.1.3.	Ensured OPSEC vulnerability reports are forwarded to HQ AIA IO Threat Analysis Center in a timely manner? *AFI 10-701, Para 3.2.1.14. and 3.3.1.12.; AFSOCI 10-701, Para* ***3.2.2.16.***			
5.1.4.	Accomplished a program assessment of their assigned unit's OPSEC programs using AFI 10-701, AFSOCI 10-701 and the self-assessment checklist located in **Attachment 3** biennially (every two years)? *AFSOCI 10-701, Para* ***3.1.4.2.*** *and* ***3.2.2.13.***			
5.2.	Has the OPSEC coordinator (below wing-level or within HQ directorates):			
5.2.1.	Reported annual OPSEC self-assessments findings to wing-level or equivalent OPSEC PM (HQ AFSOC OPSEC PM for directorates) NLT 1 October (15 October for directorates) of each year? *AFI 10-701, Para 3.2.1.11., 3.3.1.9. and Chapter 5, Table 2, OPSEC Assessment Types; AFSOCI 10-701, Para* ***3.3.1.12.*** *and* ***3.3.2.12.***			
5.2.2.	Forwarded self-assessment findings containing:			
5.2.2.1.	Training metrics for all subordinate units. *AFI 10-701, Para 2.2.2.14. and 4.1.1.3.; AFSOCI 10-701, Para* ***3.2.1.15.***			
5.2.2.2.	Number of vulnerability reports forwarded to the IO Threat Analysis Center. *AFI 10-701, Para 2.2.2.14.; AFSOCI 10-701, Para* ***3.2.1.15.***			

OPERATIONS SECURITY (OPSEC) SELF-ASSESSMENT CHECKLIST				
TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA **OPERATIONS SECURITY**	**OPR**	**DATE**		
NO.	**ITEM** ***(All references are to AFI 10-701 unless otherwise stated)***	**YES**	**NO**	**N/A**
5.2.2.3.	Number and type of survey/assessment received by subordinate units (command survey, TMAP, MDVA, Web Risk Assessments, etc.), *AFI 10-701, Para 2.2.2.14.; AFSOCI 10-701, Para* ***3.2.1.15.*** and			
5.2.2.4.	Any other information deemed of OPSEC importance. *AFI 10-701, Para 2.2.2.14., 3.2.1.11. and 3.3.1.9.; AFSOCI 10-701, Para* ***3.2.1.15.***			
5.2.3	Submitted OPSEC vulnerability reports to the wing OPSEC PM (HQ AFSOC OPSEC PM for directorates) for submission? *AFI 10-701, Para 3.2.1.14. and 3.3.1.12.; AFSOCI 10-701, Para* ***3.3.1.14.*** *and* ***3.3.2.14.***			

Attachment 4

EXAMPLE OF ATTACHMENT # TO DD FORM 254 FOR OPERATIONS SECURITY

1. This section outlines the requirements and procedures necessary for contractors to provide Operations Security (OPSEC) protection for AFSOC's critical information.

2. OPSEC is the process of identifying, analyzing and controlling critical information indicating friendly actions attendant to military operations and other activities to:

   a. Identify those actions that can be observed by adversary intelligence systems.

   b. Determine what indicators adversary intelligence systems might obtain that could be interpret or pieced together to derive critical information in time to be useful to adversaries.

   c. Select and execute countermeasures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

3. OPSEC principles are used to help assigned personnel:

   a. Maintain a continuing awareness of adversary interest in SOF actions and adversary intelligence collection capabilities.

   b. To understand the need to identify and protect classified and unclassified indicators that reveal sensitive information.

   c. To evaluate the effectiveness of OPSEC measures taken to preclude or reduce adversary acquisition and exploitation of sensitive information.

4. Our objectives are to:

   a. Protect planned operational activities by preventing the inadvertent disclosure of unclassified information relating to or revealing a possible classified operation.

   b. To preserve secrecy concerning specific scenario events and a USSOCOM or AFSOC response to these events.

   c. To identify OPSEC vulnerabilities and recommend protective measures which will serve to enhance the security of future operations.

5. AFSOC employed contractors will be provided unit-specific OPSEC education training by the assigned unit/directorate's OPSEC program manager/coordinator on the unit/directorate's OPSEC requirements before being given full access to or around an AFSOC installation, organization, facility or information, but not more than 30 days prior to initial access. Individual training will be developed and applied as required by the level of contact with AFSOC critical information.

6. OPSEC requirements, critical information lists and assistance can be found at the following:

   a. For AFSOC reference AFI 10-701 or contact the HQ AFSOC OPSEC Program Manager, AFSOC/A3I at 850 884-6326, DSN 579.

   b. For the 16th Special Operations Wing reference HFI 10-1101 or contact the Hurlburt Field OPSEC Officer, 16 SOW/IO at 850 884-4565, DSN 579.